

Short average distribution of a prime counting function over families of elliptic curves

Sumit Giri

ABSTRACT

Let E be an elliptic curve defined over \mathbb{Q} and let N be a positive integer. Now, $M_E(N)$ counts the number of primes p such that the group $E_p(\mathbb{F}_p)$ is of order N . In an earlier joint work with Balasubramanian, we showed that $M_E(N)$ follows Poisson distribution when an average is taken over a family of elliptic curve with parameters A and B where $A, B \geq N^{\frac{\ell}{2}}(\log N)^{1+\gamma}$ and $AB > N^{\frac{3\ell}{2}}(\log N)^{2+\gamma}$ for a fixed integer ℓ and any $\gamma > 0$. In this paper we show that for sufficiently large N , the same result holds even if we take A and B in the range $\exp(N^{\frac{\epsilon^2}{20\ell}}) \geq A, B > N^\epsilon$ and $AB > N^{\frac{3\ell}{2}}(\log N)^{6+\gamma}$ for any $\epsilon > 0$.

1. Introduction

Let E be an elliptic curve defined over the field of rationals \mathbb{Q} with discriminant Δ_E . For a prime p where E has good reduction, i.e. $p \nmid \Delta_E$, we denote by E_p the reduction of E modulo p . Let \mathbb{F}_p be the finite field with p elements and $E_p(\mathbb{F}_p)$ be the group of \mathbb{F}_p points over E_p .

For $p \nmid \Delta_E$, we know $|E_p(\mathbb{F}_p)| = p + 1 - a_p(E)$ where $a_p(E)$ is the trace of the Frobenius morphism at p . By Hasse's theorem we know $|a_p(E)| < 2\sqrt{p}$. For a fixed positive integer N , we define the following prime counting function

$$M_E(N) := \#\{p \text{ prime} : E \text{ has good reduction over } p \text{ and } |E_p(\mathbb{F}_p)| = N\}. \quad (1.1)$$

Now, for a pair of integers (a, b) , let $E_{a,b}$ be the elliptic curve defined by the Weierstrass equation

$$E_{a,b} : y^2 = x^3 + ax + b.$$

Also, for $A, B > 0$, we define the family of curves $\mathcal{C}(A, B)$ by

$$\mathcal{C}(A, B) := \{E_{a,b} : |a| \leq A, |b| \leq B, \Delta(E_{a,b}) \neq 0\}. \quad (1.2)$$

Now, let us recall Barban-Davenport-Halberstam conjecture for primes in arithmetic progression in short interval.

CONJECTURE 1. (Barban-Davenport-Halberstam) Let $\theta(x; q, a) = \sum_{p \leq x, p \equiv a \pmod{q}} \log p$. Let $0 < \eta \leq 1$ and $\beta > 0$ be real numbers. Suppose that X, Y , and Q are positive real numbers satisfying $X^\eta \leq Y \leq X$ and $Y/(\log X)^\beta \leq Q \leq Y$. Then

$$\sum_{q \leq Q} \sum_{\substack{1 \leq a \leq q \\ (a, q) = 1}} |\theta(X + Y; q, a) - \theta(X; q, a) - \frac{Y}{\phi(q)}|^2 \ll_{\eta, \beta} YQ \log X.$$

Under the above conjecture, David and Smith proved that

THEOREM A. *Let Conjecture 1 be true for some $0 < \eta < \frac{1}{2}$. If $A, B \geq \sqrt{N}(\log N)^{1+\gamma} \log \log N$ and that $AB \geq N^{\frac{3}{2}}(\log N)^{2+\gamma} \log \log N$, then for any odd integer N , we have*

$$\frac{1}{\#\mathcal{C}(A, B)} \sum_{E \in \mathcal{C}(A, B)} M_E(N) = \frac{K(N)N}{\phi(N) \log N} + O\left(\frac{1}{(\log N)^{1+\gamma}}\right), \quad (1.3)$$

with

$$K(N) := \prod_{p \nmid N} \left(1 - \frac{\left(\frac{N-1}{p}\right)^2 p + 1}{(p-1)^2(p+1)}\right) \prod_{p \mid N} \left(1 - \frac{1}{p^{\nu_p(N)}(p-1)}\right), \quad (1.4)$$

where ν_p denotes the usual p -adic valuation where $\nu_p(n)$ and $\left(\frac{n-1}{p}\right)$ is the Kronecker symbol.

Also, by taking another average over $N \leq x$, a similar result was unconditionally proven by Chandee, David, Koukoulopoulos and Smith [CDKS14].

Improving a result of Martin, Pollack and Smith [MPS14], in a work with Balasubramanian [BG14], we showed that the function $\frac{K(N)N}{\phi(N)}$ is 1 on an average and the average approaches 1 reasonably fast.

Using an approach first used by Banks and Shparlinski [BS09], Balog, Cojocaru and David [BCD11], Akbary and Felix [AF15], in [Par16] Parks proved that the average result in *Theorem A* is true even if we significantly relax the lower bound conditions on A and B . To be precise, he proved

THEOREM B. *Let $\epsilon, \gamma > 0$ and assume for intervals of length N^η that the Barban- Davenport- Halberstam Conjecture holds for*

$$\eta = \frac{1}{2} - (\gamma + 2) \frac{\log \log N}{\log N}.$$

Suppose further that

$$\exp(N^{\frac{\epsilon^2}{20}}) \gg A, B > N^\epsilon \text{ and } AB > N^{\frac{3}{2}}(\log N)^{6+2\gamma} \log \log N.$$

Then, for any odd integer N ,

$$\frac{1}{\mathcal{C}(A, B)} \sum_{E \in \mathcal{C}(A, B)} M_E(N) = \frac{K(N)N}{\phi(N) \log N} + O\left(\frac{1}{(\log N)^{1+\gamma}}\right),$$

where $K(N)$ is given in (1.4).

In an earlier work with Balasubramanian [BG15], we proved results related to distribution of the function $M_E(N)$. More precisely, we proved that

THEOREM C. *Let $\mathcal{C}(A, B)$ be as defined as in (1.2) and N be a positive integer greater than 7. If L be a positive integer such that $A, B > N^{L/2}(\log N)^{1+\gamma}$ and $AB > N^{3L/2}(\log N)^{2+\gamma}$ for some $\gamma > 0$, then for $1 \leq \ell \leq L - 1$*

$$\frac{1}{\#\mathcal{C}(A, B)} \sum_{\substack{E \in \mathcal{C}(A, B) \\ M_E(N) = \ell}} 1 = \frac{1}{\ell!} \left(\frac{1}{\#\mathcal{C}(A, B)} \sum_{E \in \mathcal{C}(A, B)} M_E(N) \right)^\ell \left(1 + O\left(\frac{N}{\phi(N) \log N}\right) \right) + O\left(\frac{1}{N^{\frac{L-\ell}{2}}(\log N)^\gamma}\right),$$

where the ‘ O ’ constant in the last error term is independent of γ .

Using an approach similar to Parks [Par15, Par16], in this paper, we improve *Theorem C* as follows:

THEOREM 1. *Let $0 < \epsilon < 1$ be a small positive number and ℓ be a positive integer. Suppose $\frac{\log N}{\log \log N} \geq \frac{20\ell}{\epsilon^2}$ and $\exp\left(N^{\frac{\epsilon^2}{20\ell}}\right) \gg A, B > N^\epsilon$ and $AB > N^{\frac{3\ell}{2}}(\log N)^{6+2\gamma}(\log \log N)^{\frac{\ell}{2}}$, then*

$$\frac{1}{\mathcal{C}(A, B)} \sum_{\substack{E \in \mathcal{C}(A, B) \\ M_E(N) = \ell}} 1 = \frac{1}{\ell!} \left(\frac{1}{\mathcal{C}(A, B)} \sum_{E \in \mathcal{C}(A, B)} M_E(N) \right)^\ell \left(1 + O\left(\frac{N}{\phi(N) \log N}\right) \right) + O\left(\frac{1}{(\log N)^{\ell+\gamma}}\right),$$

where the ‘ O ’ constant in the last error term is independent of γ .

Alternatively, under Conjecture 1, we can state the above theorem in the following form:

THEOREM 2. *Suppose Conjecture 1 be true for some $\eta < \frac{1}{2}$. Let γ_1 be a non negative integer and $\gamma_2 > 0$. Also let $\exp\left(N^{\frac{\epsilon^2}{20(\ell+\gamma_1)}}\right) \gg A, B > N^\epsilon$ and $AB > N^{\frac{3(\ell+\gamma_1)}{2}}(\log N)^{6+2\gamma_2}(\log \log N)^{\frac{\ell+\gamma_1}{2}}$ for a odd positive integer N with $\frac{\log N}{\log \log N} \geq \frac{20(\ell+\gamma_1)}{\epsilon^2}$. Then, for $r \leq \ell$*

$$\frac{1}{\#\mathcal{C}(A, B)} \sum_{E \in \mathcal{C}(A, B)} \sum_{M_E(N) \geq \ell} M_E(N)^r = \sum_{m=\ell}^{\ell+\gamma_1} d_{\ell, r}(m) \left(\frac{K(N)N}{\phi(N) \log N} \right)^m + O\left(\frac{N}{\phi(N) \log N}\right)^{1+\ell+\gamma_1} + O\left(\frac{1}{(\log N)^{\ell+\gamma_2}}\right),$$

where $\mathcal{C}(A, B)$ is as before and

$$d_{\ell, r}(m) = \sum_{k=\ell}^m \frac{k^r (-1)^{m-k}}{k! (m-k)!}. \quad (1.5)$$

Remark: Although, in [Par16], Theorem *B* is claimed to hold for $\exp(N^\epsilon) \gg A, B > N^\epsilon$, the correct upper bound for A and B should be of the order $\exp(N^{O(\epsilon^2)})$.

The crucial difference between proof of Theorem 1 and Theorem C is Proposition 1, which is stated in Section 3. In this proposition, we have better estimate of the number of curves of the form $E_{a,b} : y^2 = x^3 + ax + b$ with $a, b \in \mathbb{Z}$, which simultaneously reduces modulo a given set of distinct primes $(p_1, p_2, \dots, p_\ell)$ to fixed set of curves of the form $E_{s_1, t_1}/\mathbb{F}_{p_1}, E_{s_2, t_2}/\mathbb{F}_{p_2}, \dots, E_{s_\ell, t_\ell}/\mathbb{F}_{p_\ell}$ for $(s_1, s_2, \dots, s_\ell), (t_1, t_2, \dots, t_\ell) \in \mathbb{F}_{p_1}^* \times \dots \times \mathbb{F}_{p_\ell}^*$

In our previous paper with Balasubramanian [BG15], we estimated number of curves satisfying above conditions using a technique essentially due to Fouvry and Murty [FM96], which involves partitioning a rectangle of size $A \times B$ into boxes of size $p_1 p_2 \dots p_\ell \times p_1 p_2 \dots p_\ell$ and using Chinese remainder theorem to merge congruence condition over different primes together. While in Proposition 1 we use estimates of sums of suitable multiplicative characters.

Acknowledgements: I would like to thank Chantal David, Dimitris Koukoulopoulos and Amir Akbary for their useful advices. I also thank James Parks for spending time in clarifying some of my doubts that were essential for completing the work.

Funding: This work was done while working as a Postdoctoral Fellow at Centre de Recherches Mathematiques, Universit de Montreal.

2. Preliminaries

Let D be a negative discriminant. Using the class number formula [p. 515, [IK]], the *Kronecker class number* for a discriminant D can be written as

$$H(D) := \sum_{\substack{f^2 | D \\ D/f^2 \equiv 0,1 \pmod{4}}} \frac{\sqrt{|D|}}{2\pi f} L(1, \chi_{D/f^2}) \quad (2.1)$$

where χ_d is the Kronecker symbol $(\frac{d}{\cdot})$ and $L(s, \chi_d) := \sum_{n=1}^{\infty} \frac{\chi_d(n)}{n^s}$.

Using Deuring's theorem [Deu41] we get

$$H(t^2 - 4p) = \sum_{\substack{\tilde{E}/\mathbb{F}_p \\ \alpha_p(E)=t}} \frac{1}{\#\text{Aut}(\tilde{E})}, \quad (2.2)$$

where the sum is over the F_p -isomorphism classes of elliptic curves.

Define,

$$\begin{aligned} D_N(p) &:= (p+1-N)^2 - 4p = (N+1-p)^2 - 4N, \\ N^+ &:= (\sqrt{N}+1)^2; \quad N^- := (\sqrt{N}-1)^2 \\ d_{N,f}(p) &:= \frac{D_N(p)}{f^2} \text{ for } f^2 \mid D_N(p). \end{aligned} \quad (2.3)$$

With these notations defined, we recall the following lemma from [Lemma 2.1, [BG15]]

LEMMA 1. *Let N be a positive integers and N^- and N^+ are defined as above. Also let $H(D_N(p))$ be defined by (2.1) and (2.3). Then*

(a)

$$\sum_{N^- < p < N^+} H(D_N(p)) \ll \frac{N^2}{\phi(N) \log N}.$$

(b) For $k \geq 2$,

$$\sum_{N^- < p < N^+} H(D_N(p))^k \ll N^{\frac{k+1}{2}} (\log N)^{k-2} (\log \log N)^k.$$

We also need the following two theorems:

THEOREM 3. *Let M, N, Q be positive integers and let $\{a_n\}_n$ is a sequence of complex numbers. For a fixed $q \leq Q$, we let χ be a Dirichlet character modulo q . Then*

$$\sum_{q \leq Q} \frac{q}{\phi(q)} \sum_{\substack{\chi \pmod{q} \\ \chi \text{ primitive}}} \left| \sum_{M < n \leq M+N} a_n \chi(n) \right|^2 \leq (N + 3Q^2) \sum_{M < n \leq M+N} |a_n|^2.$$

For the proof of the above theorem, see [Chapter 27, [Dav00]].

The second theorem is due to Friedlander and Iwaniec [FI2], which bounds the fourth power moment of Dirichlet characters.

THEOREM 4. (**Friedlander-Iwaniec**) Let q and N be positive integers. Let χ denote a Dirichlet character modulo q , with χ_0 denoting the principal character. Then

$$\sum_{\chi \neq \chi_0} \left| \sum_{n \leq N} \chi(n) \right|^4 \ll N^2 q \log^6 q.$$

3. Proof of Theorems

Let $r \geq 1$ be a positive integer. We have,

$$\begin{aligned} \frac{1}{\#\mathcal{C}(A, B)} \sum_{\substack{E \in \mathcal{C}(A, B) \\ M_E(N) \geq \ell}} M_E(N)^r &= \frac{1}{\#\mathcal{C}(A, B)} \sum_{\substack{E \in \mathcal{C}(A, B) \\ M_E(N) \geq \ell}} \left(\sum_{\substack{N^- < p < N^+ \\ E_p(\mathbb{F}_p) = N}} 1 \right)^r \\ &= \frac{1}{\#\mathcal{C}(A, B)} \sum_{N^- < p_1, \dots, p_r < N^+} \sum_{\substack{E \in \mathcal{C}(A, B), M_E(N) \geq \ell \\ E_{p_1}(\mathbb{F}_{p_1}) = \dots = E_{p_r}(\mathbb{F}_{p_r}) = N}} 1. \end{aligned}$$

For any non-negative integer γ_1 , breaking the sum into two parts, the right hand side can be written as

$$\frac{1}{\#\mathcal{C}(A, B)} \sum_{\substack{N^- < p_i < N^+ \\ 1 \leq i \leq r}} \sum_{j=\ell}^{\ell+\gamma_1} \sum_{\substack{M_E(N)=j \\ E_{p_i}(\mathbb{F}_{p_i})=N \\ E \in \mathcal{C}(A, B), 1 \leq i \leq r}} 1 + \frac{1}{\#\mathcal{C}(A, B)} \sum_{\substack{N^- < p_i < N^+ \\ 1 \leq i \leq r}} \sum_{\substack{M_E(N) \geq \ell+\gamma_1+1 \\ E_{p_i}(\mathbb{F}_{p_i})=N \\ E \in \mathcal{C}(A, B), 1 \leq i \leq r}} 1 \quad (3.1)$$

For $r \leq \ell$, consider the expression

$$\frac{1}{\#\mathcal{C}(A, B)} \sum_{\substack{N^- < p_i < N^+ \\ 1 \leq i \leq r}} \sum_{\substack{E \in \mathcal{C}(A, B) \\ M_E(N) \geq \ell+1 \\ E_{p_i}(\mathbb{F}_{p_i})=N \\ 1 \leq i \leq r}} 1 \quad (3.2)$$

Now, for a curve E with $M_E(N) = L \geq \ell + 1$, the curve E is counted L^r times in (3.2). While, the same E is counted $\frac{L!}{(L-\ell-1)!}$ times if we consider the expression

$$\frac{1}{\#\mathcal{C}(A, B)} \sum_{\substack{N^- < p_i < N^+ \\ 1 \leq i \leq \ell+1 \\ p_m \neq p_n \text{ for } m \neq n}} \sum_{\substack{E \in \mathcal{C}(A, B) \\ E_{p_i}(\mathbb{F}_{p_i})=N \\ 1 \leq i \leq \ell+1}} 1 \quad (3.3)$$

Using Stirling's approximation, is easy to see that $\frac{L^r(L-\ell-1)!}{L!} \ll e^\ell$ for $r \leq \ell$. Thus

$$\frac{1}{\#\mathcal{C}(A, B)} \sum_{\substack{N^- < p_i < N^+ \\ 1 \leq i \leq r}} \sum_{\substack{E \in \mathcal{C}(A, B) \\ M_E(N) \geq \ell+\gamma_1+1 \\ E_{p_i}(\mathbb{F}_{p_i})=N \\ 1 \leq i \leq r}} 1 \ll_{\ell, \gamma_1} \frac{1}{\#\mathcal{C}(A, B)} \sum_{\substack{N^- < p_i < N^+ \\ 1 \leq i \leq \ell+\gamma_1+1 \\ p_m \neq p_n, \forall m \neq n}} \sum_{\substack{E \in \mathcal{C}(A, B) \\ E_{p_i}(\mathbb{F}_{p_i})=N \\ 1 \leq i \leq \ell+\gamma_1+1}} 1 \quad (3.4)$$

For $r \leq \ell \leq j \leq \ell + \gamma_1$, using a similar argument, one can also show that

$$\frac{1}{\#\mathcal{C}(A, B)} \sum_{\substack{N^- < p_i < N^+ \\ 1 \leq i \leq r}} \sum_{\substack{M_E(N)=j \\ E_{p_i}(\mathbb{F}_{p_i})=N \\ E \in \mathcal{C}(A, B), 1 \leq i \leq r}} 1 = \frac{j^r}{j!} \frac{1}{\#\mathcal{C}(A, B)} \sum_{\substack{N^- < p_i < N^+ \\ 1 \leq i \leq j \\ pm \neq pn \text{ for } m \neq n}} \sum_{\substack{E \in \mathcal{C}(A, B) \\ E_{p_i}(\mathbb{F}_{p_i})=N \\ 1 \leq i \leq j, M_E(N)=j}} 1 \quad (3.5)$$

Also, for $r \leq \ell \leq j \leq \ell + \gamma_1$,

$$\sum_{\substack{N^- < p_i < N^+ \\ 1 \leq i \leq r \\ pm \neq pn \text{ for } m \neq n}} \sum_{\substack{E \in \mathcal{C}(A, B) \\ E_{p_i}(\mathbb{F}_{p_i})=N \\ 1 \leq i \leq r, M_E(N)=j}} 1 = \frac{1}{(j-r)!} \sum_{\substack{N^- < p_i < N^+ \\ 1 \leq i \leq j \\ pm \neq pn \text{ for } m \neq n}} \sum_{\substack{E \in \mathcal{C}(A, B) \\ E_{p_i}(\mathbb{F}_{p_i})=N \\ 1 \leq i \leq j, M_E(N)=j}} 1 \quad (3.6)$$

We now consider the first term of (3.1). Note that, the primes in the range of summations in (3.1) are not distinct. Recalling the definition of $S(n, m)$, the Stirling number of the second kind, which equals to the number of ways of partitioning a set of n elements into m non empty sets, we get

$$\sum_{\substack{N^- < p_i < N^+ \\ 1 \leq i \leq r}} \sum_{\substack{E \in \mathcal{C}, M_E(N)=j \\ E(\mathbb{F}_{p_1})=\dots=E(\mathbb{F}_{p_r})=N}} 1 = \left(\sum_{m=1}^r \frac{S(r, m)}{(j-m)!} \right) \sum_{\substack{N^- < p_i < N^+ \\ 1 \leq i \leq r}} \sum_{\substack{E \in \mathcal{C}(A, B), M_E(N)=j \\ E_{p_1}(\mathbb{F}_{p_1})=\dots=E_{p_r}(\mathbb{F}_{p_r})=N}} 1. \quad (3.7)$$

To simplify the first factor on the right hand side, we use the equality $\sum_{m=1}^r \frac{S(r, m)j!}{(j-m)!} = j^r$. See [(4.1.3), p. 60, [Rom84]].

With this,

$$\begin{aligned} & \sum_{\substack{N^- < p_1 \neq p_2 \neq \dots \neq p_j < N^+ \\ E \in \mathcal{C}(A, B), M_E(N)=j \\ E_{p_1}(\mathbb{F}_{p_1})=\dots=E_{p_r}(\mathbb{F}_{p_r})=N}} 1 \\ &= \sum_{\substack{N^- < p_1 \neq p_2 \neq \dots \neq p_j < N^+ \\ E \in \mathcal{C}(A, B), M_E(N) \geq j \\ E(\mathbb{F}_{p_1})=\dots=E(\mathbb{F}_{p_j})=N}} \sum_{\substack{E \in \mathcal{C}(A, B), M_E(N)=j \\ E_{p_1}(\mathbb{F}_{p_1})=\dots=E_{p_r}(\mathbb{F}_{p_r})=N}} 1 - \sum_{\substack{N^- < p_1 \neq p_2 \neq \dots \neq p_j < N^+ \\ E \in \mathcal{C}(A, B), M_E(N) \geq j+1 \\ E(\mathbb{F}_{p_1})=\dots=E(\mathbb{F}_{p_j})=N}} \sum_{\substack{E \in \mathcal{C}(A, B), M_E(N)=j \\ E_{p_1}(\mathbb{F}_{p_1})=\dots=E_{p_r}(\mathbb{F}_{p_r})=N}} 1 \end{aligned} \quad (3.8)$$

Now we denote the left hand side of (3.6) by $\omega(r, j)$ and the first term of the right hand side of (3.8) by $\Omega(j, j)$. Also we call the left hand side of (3.7) by $\Upsilon(r, j)$. Then, in view of (3.6) and (3.7), we get the following set of relations

$$\begin{cases} \Upsilon(r, j) = \frac{j^r}{j!} \omega(j, j), \\ \Omega(t, s) = \sum_{n=s}^{\infty} \omega(t, n) \quad \text{for } t \leq s, \\ \omega(t, n) = \frac{1}{(n-t)!} \omega(n, n) \quad \text{for } t \leq n. \end{cases} \quad (3.9)$$

Now, we state the following Proposition, whose proof will be completed in Section 4.

PROPOSITION 1. *Let $\mathcal{C}(A, B)$ be as above. Let $0 < \epsilon < 1$ be a small positive number. Suppose N be a positive integer such that $\frac{\log N}{\log \log N} \geq \frac{20\ell}{\epsilon^2}$ with $\exp\left(\left(\frac{N}{\log N}\right)^{\frac{\epsilon^2}{20\ell}}\right) \gg A, B > N^\epsilon$ and*

$AB > N^{\frac{3\ell}{2}}(\log N)^{6+2\gamma_2}(\log \log N)^{\frac{\ell}{2}}$, then

$$\frac{1}{\#\mathcal{C}(A, B)} \sum_{\substack{N^- < p_i < N^+ \\ 1 \leq i \leq \ell \\ pm \neq pn \text{ for } m \neq n}} \sum_{\substack{E \in \mathcal{C}(A, B) \\ Ep_i(\mathbb{F}_{p_i}) = N \\ 1 \leq i \leq \ell}} 1 = \left(\sum_{N^- < p < N^+} \frac{H(D_N(p))}{p} \right)^\ell + O\left(\frac{1}{(\log N)^{\ell+\gamma_2}}\right).$$

Now, by Proposition 1

$$\frac{1}{\#\mathcal{C}(A, B)} \Omega(j, j) = \left(\sum_{N^- < p < N^+} \frac{H(D_N(p))}{p} \right)^j + O\left(\frac{1}{(\log N)^{j+\gamma_2}}\right),$$

whenever $\exp\left(\left(\frac{N}{\log N}\right)^{\frac{\ell^2}{20\ell}}\right) \gg A, B > N^\epsilon$ and $AB > N^{\frac{3\ell}{2}}(\log N)^{6+2\gamma_2}$.

Now, we replace $\sum_{j=\ell}^{\ell+\gamma_1} \Upsilon(r, j)$ by $\sum_{j=\ell}^{\ell+\gamma_1} z_{\ell,r}(j) \Omega(j, j) + O(\Omega(\ell + \gamma_1, \ell + \gamma_1 + 1))$ where $\{z_{\ell,r}(j)\}$ are some constants to be determined later using (3.9). Also note that $\Omega(\ell + \gamma_1, \ell + \gamma_1 + 1) \ll AB \left[\left(\sum_p \frac{H(D_N(p))}{p} \right)^{\ell+\gamma_1} + \frac{1}{(\log N)^{\ell+\gamma_2}} \right]$.

Then, in view of (3.4) and Proposition 1, the expression in (3.1) equals to

$$\sum_{j=\ell}^{\ell+\gamma_1} z_{\ell,r}(j) \left(\sum_{N^- < p < N^+} \frac{H(D_N(p))}{p} \right)^j + O\left(\sum_{N^- < p < N^+} \frac{H(D_N(p))}{p} \right)^{\ell+\gamma_1+1} + O\left(\frac{1}{(\log N)^{\ell+\gamma_2}}\right) \quad (3.10)$$

for some real numbers $\{z_{\ell,r}(j)\}_{j=\ell}^{\ell+\gamma_1}$

Only thing that remains to be shown is that $\{z_{\ell,r}(j)\}_j$ are equals to $\{d_{\ell,r}(j)\}_j$, as defined in (1.5). For that, we have the following lemma.

LEMMA 2. Consider ω, Ω as variables satisfying the identities in (3.9). Then, the solution of the equation

$$\sum_{j=\ell}^{\infty} \frac{j^r}{j!} \omega(j, j) = \sum_{j=\ell}^{\infty} z_{\ell,r}(j) \Omega(j, j)$$

in variables $z_{\ell,r}(j)$ are given by

$$z_{\ell,r}(j) = \sum_{k=\ell}^j \frac{k^r}{k!} \frac{(-1)^{j-k}}{(j-k)!} = d_{\ell,r}(j).$$

Proof. See [Lemma 3.2, [BG15]] for the proof of the above lemma. □

Finally, combining (3.2), (3.10) and Lemma 2, we have

$$\begin{aligned} \frac{1}{\#\mathcal{C}(A, B)} \sum_{\substack{E \in \mathcal{C}(A, B) \\ M_E(N) \geq \ell}} M_E(N)^r &= \sum_{j=\ell}^{\ell+\gamma_1} d_{\ell, r}(j) \left(\sum_{N^- < p < N^+} \frac{H(D_N(p))}{p} \right)^j \\ &\quad + O \left(\sum_{N^- < p < N^+} \frac{H(D_N(p))}{p} \right)^{\ell+\gamma_1+1} + O \left(\frac{1}{(\log N)^{\ell+\gamma_2}} \right) \end{aligned} \quad (3.11)$$

for $\exp \left(\left(\frac{N}{\log N} \right)^{\frac{\epsilon^2}{20(\ell+\gamma_1)}} \right) \gg A, B > N^\epsilon$ and $AB > N^{\frac{3(\ell+\gamma_1)}{2}} (\log N)^{6+\gamma_2}$.

Putting $\ell = 1$, $r = 1$ and $\gamma_1 = 0$, $\gamma_2 = \gamma$, from (3.11) we get,

$$\begin{aligned} \frac{1}{\#\mathcal{C}(A, B)} \sum_{E \in \mathcal{C}(A, B)} M_E(N) &= \sum_{N^- < p < N^+} \frac{H(D_N(p))}{p} + O \left(\left(\sum_{N^- < p < N^+} \frac{H(D_N(p))}{p} \right)^2 \right) \\ &\quad + O \left(\frac{1}{(\log N)^{1+\gamma}} \right) \end{aligned} \quad (3.12)$$

for $\exp \left(\left(\frac{N}{\log N} \right)^{\frac{\epsilon^2}{20}} \right) \gg A, B > N^\epsilon$ and $AB > N^{\frac{3}{2}} (\log N)^{6+\gamma}$

Also, for $\gamma_1 = 0$, $\gamma_2 = \gamma$, from (3.11) we have

$$\begin{aligned} \frac{1}{\#\mathcal{C}(A, B)} \sum_{\substack{E \in \mathcal{C}(A, B) \\ M_E(N) = \ell}} M_E(N)^r &= d_{\ell, r}(\ell) \left(\sum_{N^- < p < N^+} \frac{H(D_N(p))}{p} \right)^\ell + O \left(\sum_{N^- < p < N^+} \frac{H(D_N(p))}{p} \right)^{\ell+1} \\ &\quad + O \left(\frac{1}{(\log N)^{\ell+\gamma}} \right) \end{aligned}$$

or,

$$\begin{aligned} \frac{1}{\#\mathcal{C}(A, B)} \sum_{\substack{E \in \mathcal{C}(A, B) \\ M_E(N) = \ell}} 1 &= \frac{d_{\ell, r}(\ell)}{\ell^r} \left(\sum_{N^- < p < N^+} \frac{H(D_N(p))}{p} \right)^\ell + O \left(\sum_{N^- < p < N^+} \frac{H(D_N(p))}{p} \right)^{\ell+1} \\ &\quad + O \left(\frac{1}{(\log N)^{\ell+\gamma}} \right) \end{aligned} \quad (3.13)$$

for $\exp \left(\left(\frac{N}{\log N} \right)^{\frac{\epsilon^2}{20\ell}} \right) \gg A, B > N^\epsilon$ and $AB > N^{\frac{3\ell}{2}} (\log N)^{6+\gamma}$.

We use (3.12) and (3.13) to replace $\sum_{N^- < p < N^+} \frac{H(D_N(p))}{p}$ in the right hand side of (3.13) by

$\frac{1}{\#\mathcal{C}(A,B)} \sum_{E \in \mathcal{C}(A,B)} M_E(N)$. Now, using Lemma 1a, we get

$$\begin{aligned} \frac{1}{\#\mathcal{C}(A,B)} \sum_{\substack{E \in \mathcal{C}(A,B) \\ M_E(N)=\ell}} 1 &= \frac{d_{\ell,r}}{\ell^r}(\ell) \left(\frac{1}{\#\mathcal{C}(A,B)} \sum_{E \in \mathcal{C}(A,B)} M_E(N) \right)^\ell \left(1 + O\left(\frac{N}{\varphi(N) \log N} \right) \right) \\ &\quad + O\left(\frac{1}{(\log N)^{\ell+\gamma}} \right) \end{aligned}$$

for $\exp\left(\left(\frac{N}{\log N}\right)^{\frac{2}{20\ell}}\right) \gg A, B > N^\epsilon$ and $AB > N^{\frac{3\ell}{2}}(\log N)^{6+\gamma}$. Further, we recall that $d_{\ell,r}(\ell) = \frac{\ell^r}{\ell!}$. This proves Theorem 1.

Assuming Conjecture 1 and the proof of [Theorem 3, [DS13]], we have that

$$\sum_{N^- < p < N^+} \frac{H(D_N(p))}{p} = \frac{K(N)N}{\varphi(N) \log N} + O\left(\frac{1}{(\log N)^{1+\gamma}}\right) \quad (3.14)$$

for odd integer N , where $K(N)$ is given by (1.4). Combining (3.14) with (3.11), we complete the proof of Theorem 2.

4. Proof of Proposition 1

Before proceeding with the proof of the proposition, we define some standard notations.

Let $P := (p_1, \dots, p_\ell)$ be a vector of ℓ distinct primes such that $(\sqrt{N} - 1)^2 < p_i < (\sqrt{N} + 1)^2$ for $1 \leq i \leq \ell$. So, the primes in question are effectively of the order N .

Let $S := (s_1, \dots, s_\ell)$ and $T := (t_1, \dots, t_\ell)$ be elements of $\mathbb{F}_{p_1}^* \times \mathbb{F}_{p_2}^* \times \dots \times \mathbb{F}_{p_\ell}^*$. For such S and T as above, define the following indicator function

$$h(P, N, S, T) := \begin{cases} 1 & \text{if } \#E_{p_i, s_i, t_i}(\mathbb{F}_{p_i}) = N \text{ for } 1 \leq i \leq \ell, \\ 0 & \text{otherwise.} \end{cases} \quad (4.1)$$

Also,

$$\sum_{S, T \in \mathbb{F}(P)} 1 = \sum_{\substack{1 \leq s_1 \leq p_1 \\ 1 \leq t_1 \leq p_1}} \dots \sum_{\substack{1 \leq s_\ell \leq p_\ell \\ 1 \leq t_\ell \leq p_\ell}} 1 \quad \text{and} \quad \sum_{S, T \in \mathbb{F}(P)^*} 1 = \sum_{\substack{1 \leq s_1 < p_1 \\ 1 \leq t_1 < p_1}} \dots \sum_{\substack{1 \leq s_\ell < p_\ell \\ 1 \leq t_\ell < p_\ell}} 1.$$

Throughout the rest of the proof, $E_{s,t} : y^2 = x^3 + sx + t$ denotes a curve over a finite field \mathbb{F}_p . Also $E_{a,b}$ denotes curve over \mathbb{Q} as defined in (1.2).

Further, we know, two elliptic curves $E_{s,t}$ and $E_{s',t'}$ are isomorphic over \mathbb{F}_p if and only if there exists a $u \in \mathbb{F}_p^*$ such that $s' = su^4$ and $t' = tu^6$. Hence, the number of elliptic curves over \mathbb{F}_p isomorphic to $E_{s,t}$ is

$$\frac{\#\mathbb{F}_p^*}{\#\text{Aut}(E_{s,t})} = \frac{p-1}{\#\text{Aut}(E_{s,t})}.$$

Further,

$$\#\text{Aut}(E_{s,t}) = \begin{cases} 6 & \text{if } s = 0 \text{ and } p \equiv 1 \pmod{3}, \\ 4 & \text{if } t = 0 \text{ and } p \equiv 1 \pmod{4}, \\ 2 & \text{otherwise.} \end{cases}$$

For $1 \leq i \leq \ell$,

$$\sum_{\substack{1 \leq s_i, t_i \leq p_i \\ \#E_{p_i, s_i, t_i}(\mathbb{F}_{p_i})=N}} 1 = \sum_{\substack{\bar{E}_{p_i, s_i, t_i}/\mathbb{F}_{p_i} \\ p_i+1-a_{p_i}(\bar{E}_{p_i, s_i, t_i})=N}} \frac{p_i - 1}{\#\text{Aut}(\bar{E}_{p_i, s_i, t_i}(\mathbb{F}_{p_i}))}, \quad (4.2)$$

where the summation in the right hand side of (4.2) runs over isomorphism classes of elliptic curve $\bar{E}_{p_i, s_i, t_i}(\mathbb{F}_{p_i})$. Further, using (2.2), from (4.2) we get

$$\sum_{\substack{1 \leq s_i, t_i \leq p_i \\ \#E_{p_i, s_i, t_i}(\mathbb{F}_{p_i})=N}} 1 = (p_i - 1)H(D_N(p_i)) \quad (4.3)$$

Now, the left hand side of the proposition 1 is equal to

$$\begin{aligned} & \frac{1}{\#\mathcal{C}(A, B)} \sum_{\substack{N^- < p_i < N^+ \\ 1 \leq i \leq \ell \\ p_m \neq p_n, \forall m \neq n}} \sum_{\substack{E \in \mathcal{C}(A, B) \\ E_{p_i}(\mathbb{F}_{p_i})=N \\ 1 \leq i \leq \ell}} 1 \\ &= \frac{1}{\#\mathcal{C}(A, B)} \sum_{\substack{N^- < p_i < N^+ \\ 1 \leq i \leq \ell \\ p_m \neq p_n, \forall m \neq n}} \sum_{S, T \in \mathbb{F}(P)} h(P, N, S, T) \sum_{\substack{|a| \leq A, |b| \leq B \\ a \equiv s_i \pmod{p_i} \\ b \equiv t_i \pmod{p_i} \\ 1 \leq i \leq \ell}} 1. \end{aligned} \quad (4.4)$$

We plan to count the number of curves $E_{a,b} \in \mathcal{C}(A, B)$ whose reductions modulo p_i are E_{s_i, t_i} for all p_i . Then, the inner summation on left hand side of (4.4) can be written as

$$\begin{aligned} & \frac{1}{\#\mathcal{C}(A, B)} \sum_{\substack{E \in \mathcal{C}(A, B) \\ E_{p_i}(\mathbb{F}_{p_i})=N \\ 1 \leq i \leq \ell}} 1 = \frac{1}{\#\mathcal{C}(A, B)} \sum_{S, T \in \mathbb{F}(P)} h(P, N, S, T) \prod_{j=1}^{\ell} \frac{\#\text{Aut}(E_{p_j, s_j, t_j})}{(p_j - 1)} \sum_{\substack{|a| \leq A, |b| \leq B \\ \exists (u_1, \dots, u_{\ell}) \in \mathbb{F}(P)^* \\ a \equiv s_i u_i^4 \pmod{p_i}, \\ b \equiv t_i u_i^6 \pmod{p_i} \\ \forall 1 \leq i \leq \ell}} 1. \\ &= \frac{1}{\#\mathcal{C}(A, B)} \sum_{\substack{N^- < p_i < N^+ \\ 1 \leq i \leq \ell \\ p_m \neq p_n, \forall m \neq n}} \sum_{S, T \in \mathbb{F}(P)} h(P, N, S, T) Z(P, S, T) \prod_{j=1}^{\ell} \frac{\#\text{Aut}(E_{p_j, s_j, t_j})}{(p_j - 1)}, \end{aligned} \quad (4.5)$$

where $Z(P, S, T)$ denotes the number of integers $|a| \leq A, |b| \leq B$ such that $\exists (u_1, \dots, u_{\ell}) \in \mathbb{F}(P)^*$ such that

$$a \equiv s_i u_i^4 \pmod{p_i}, \quad b \equiv t_i u_i^6 \pmod{p_i} \quad \text{for } 1 \leq i \leq \ell.$$

Now, $\#\text{Aut}(\mathbf{E}_{s,t}) = 2$ most of the times and in particular when $st \neq 0$. So, we write (4.5) as

$$\begin{aligned} \frac{2^\ell}{\#\mathcal{C}(A, B)} \sum_{\substack{N^- < p_i < N^+ \\ 1 \leq i \leq \ell \\ p_m \neq p_n, \forall m \neq n}} \sum_{S, T \in \mathbb{F}(P)^*} \frac{h(P, N, S, T) Z(P, S, T)}{(p_1 - 1) \cdots (p_\ell - 1)} \\ + \frac{1}{\#\mathcal{C}(A, B)} \sum_{\substack{N^- < p_i < N^+ \\ 1 \leq i \leq \ell \\ p_m \neq p_n, \forall m \neq n \text{ for some } 1 \leq i \leq \ell}} \sum_{\substack{S, T \in \mathbb{F}(P) \\ s_i t_i = 0}} h(P, N, S, T) Z(P, S, T) \prod_{j=1}^{\ell} \frac{\#\text{Aut}(\mathbf{E}_{p_j, s_j, t_j})}{(p_j - 1)}. \end{aligned} \quad (4.6)$$

Define

$$\Sigma_1 := \frac{2^\ell}{\#\mathcal{C}(A, B)} \sum_{\substack{N^- < p_i < N^+ \\ 1 \leq i \leq \ell \\ p_m \neq p_n, \forall m \neq n}} \sum_{S, T \in \mathbb{F}(P)^*} \frac{h(P, N, S, T) Z(P, S, T)}{(p_1 - 1) \cdots (p_\ell - 1)} \quad (4.7)$$

$$\Sigma_2 := \frac{1}{\#\mathcal{C}(A, B)} \sum_{\substack{N^- < p_i < N^+ \\ 1 \leq i \leq \ell \\ p_m \neq p_n, \forall m \neq n \text{ for some } 1 \leq i \leq \ell}} \sum_{\substack{S, T \in \mathbb{F}(P) \\ s_i t_i = 0}} h(P, N, S, T) Z(P, S, T) \prod_{j=1}^{\ell} \frac{\#\text{Aut}(\mathbf{E}_{p_j, s_j, t_j})}{(p_j - 1)}. \quad (4.8)$$

We plan to complete the estimation of Σ_1 first. Later, we show that the same estimation technique can be modified suitably to give required upper bound to Σ_2 .

For this part of the proof related to the estimation of Σ_1 , we are essentially going to follow the approach of Parks [Par15], except possibly the different range of summation over primes.

Separating the expected main term from the expected error term in Σ_1 , we write

$$\begin{aligned} \Sigma_1 := & \frac{4AB}{\#\mathcal{C}(A, B)} \sum_{\substack{N^- < p_i < N^+ \\ 1 \leq i \leq \ell \\ p_m \neq p_n, \forall m \neq n}} \prod_{j=1}^{\ell} \frac{1}{p_j(p_j - 1)} \sum_{S, T \in \mathbb{F}(P)^*} h(P, N, S, T) \\ & + \frac{2^\ell}{\#\mathcal{C}(A, B)} \sum_{\substack{N^- < p_i < N^+ \\ 1 \leq i \leq \ell \\ p_m \neq p_n, \forall m \neq n}} \prod_{j=1}^{\ell} \frac{1}{(p_j - 1)} \sum_{S, T \in \mathbb{F}(P)^*} h(P, N, S, T) \left(Z(P, S, T) - \frac{4AB}{2^\ell p_1 \cdots p_\ell} \right). \end{aligned} \quad (4.9)$$

In order to bound the second summation on the right hand side of (4.9), we use the following lemma

LEMMA 3. *Let $\ell, A, B, h(\cdot), Z(\cdot)$ as defined before. Then, as $N \rightarrow \infty$, we have*

$$\begin{aligned} & \sum_{\substack{N^- < p_i < N^+ \\ 1 \leq i \leq \ell \\ p_m \neq p_n, \forall m \neq n}} \frac{1}{p_1 \cdots p_\ell} \sum_{S, T \in \mathbb{F}(P)^*} h(P, N, S, T) \left(Z(P, S, T) - \frac{AB}{2^{\ell-2} p_1 \cdots p_\ell} \right) \\ & \ll_{k, \ell} AB N^{-\frac{\ell}{4k}} (\log N)^{\frac{\ell}{2k}} (\log \log N)^\ell \left((\log A)^{\frac{k^2-1}{2k}} + (\log B)^{\frac{k^2-1}{2k}} \right) \\ & + (A\sqrt{B} + B\sqrt{A}) N^{\frac{3\ell}{4k}} (\log N)^{\frac{k^2+\ell-1}{2k}} (\log \log N)^\ell + \sqrt{AB} N^{\frac{3\ell}{4}} (\log N)^{3-\ell} (\log \log N)^{\frac{\ell}{2}}, \end{aligned} \quad (4.10)$$

for any positive integer k .

We give a proof of the above lemma later in this section.

Now, using (4.3), we write the inner summation in the first sum in (4.9) as

$$\begin{aligned}
 \sum_{S, T \in \mathbb{F}(P)^*} h(P, N, S, T) &= \sum_{\substack{1 \leq s_1, t_1 < p_1 \\ \#E_{p_1, s_1, t_1}(\mathbb{F}_{p_1}) = N}} \cdots \sum_{\substack{1 \leq s_\ell, t_\ell < p_\ell \\ \#E_{p_\ell, s_\ell, t_\ell}(\mathbb{F}_{p_\ell}) = N}} 1. \\
 &= \prod_{i=1}^{\ell} \left(\sum_{\substack{\bar{E}_{p_i, s_i, t_i} / \mathbb{F}_{p_i} \\ p_i + 1 - a_{p_i}(\bar{E}_{p_i, s_i, t_i}) = N}} \frac{p_i - 1}{\#\text{Aut}(\bar{E}_{p_i, s_i, t_i}(\mathbb{F}_{p_i}))} + O(p_i) \right) \\
 &= \prod_{i=1}^{\ell} \left((p_i - 1)H(D_N(p_i)) + O(p_i) \right). \tag{4.11}
 \end{aligned}$$

Using the bound $L(1, \chi_{d_{N,f}(p)}) \ll \log N$, one can show that $H(D_N(p_i)) \ll \sqrt{N} \log N \log \log N$ for $1 \leq i \leq \ell$. This together with (4.11) gives

$$\sum_{S, T \in \mathbb{F}(P)^*} h(P, N, S, T) = \prod_{i=1}^{\ell} (p_i - 1)H(D_N(p_i)) + O_{\ell} \left(N^{\frac{3\ell-1}{2}} (\log N)^{\ell-1} (\log \log N)^{\ell-1} \right). \tag{4.12}$$

Using (4.12), the first term in (4.9) can be written as

$$\begin{aligned}
 &\frac{4AB}{\#\mathcal{C}(A, B)} \sum_{\substack{N^- < p_i < N^+ \\ 1 \leq i \leq \ell \\ p_i \neq p_j, \forall i \neq j}} \prod_{j=1}^{\ell} \frac{1}{p_j(p_j - 1)} \sum_{S, T \in \mathbb{F}(P)^*} h(P, N, S, T) \\
 &= \frac{4AB}{\#\mathcal{C}(A, B)} \sum_{\substack{N^- < p_i < N^+ \\ 1 \leq i \leq \ell \\ p_i \neq p_j, \forall i \neq j}} \left(\prod_{j=1}^{\ell} \frac{H(D_N(p_j))}{p_j} + O_{\ell} \left(\frac{1}{N^{2\ell}} \cdot N^{\frac{3\ell-1}{2}} (\log N)^{\ell-1} (\log \log N)^{\ell-1} \right) \right) \\
 &= \left(\sum_{\substack{N^- < p_i < N^+ \\ 1 \leq i \leq \ell \\ p_m \neq p_n, \forall m \neq n}} \prod_{j=1}^{\ell} \frac{H(D_N(p_j))}{p_j} + O_{\ell} \left(\frac{(\log \log N)^{\ell-1}}{\sqrt{N} \log N} \right) \right) \left(1 + O_{\ell} \left(\frac{1}{A} + \frac{1}{B} + \frac{1}{AB} \right) \right). \tag{4.13}
 \end{aligned}$$

Combining (4.13) and Lemma 1, together with Lemma 3, we can write (4.9) as

$$\Sigma_1 = \left(\sum_{N^- < p < N^+} \frac{H(D_N(p))}{p} \right)^{\ell} + \mathcal{E}_1(N, A, B, \ell)$$

where

$$\begin{aligned}
 \mathcal{E}_1(N, A, B, \ell) &\ll_{\ell, k} N^{-\frac{\ell}{4k}} (\log N)^{\frac{\ell}{2k}} (\log \log N)^{\ell} \left((\log A)^{\frac{k^2-1}{2k}} + (\log B)^{\frac{k^2-1}{2k}} \right) + \frac{1}{\sqrt{AB}} N^{\frac{3\ell}{4}} (\log N)^{3-\ell} (\log \log N)^{\frac{\ell}{2}} \\
 &\quad + \left(\frac{1}{\sqrt{B}} + \frac{1}{\sqrt{A}} \right) N^{+\frac{3\ell}{4k}} (\log N)^{\frac{k^2+\ell-1}{2k}} (\log \log N)^{\ell} + \left(\frac{\log \log N}{\log N} \right)^{\ell} \left(\frac{1}{A} + \frac{1}{B} + \frac{1}{AB} \right) + O_{\ell}(N^{-\frac{1}{2}}). \tag{4.14}
 \end{aligned}$$

For the time being, we assume that Σ_2 is significantly small compared to $\mathcal{E}_1(N, A, B, \ell)$ under the condition that $A, B \geq N^\epsilon$. Choose $k = \frac{2\ell}{\epsilon}$. Now, if

$$\begin{aligned} N^\epsilon &\leq A, B \leq \exp(N^{\frac{\epsilon^2}{20\ell}}) \\ AB &\geq N^{\frac{3\ell}{2}} (\log N)^{6+2\gamma_2} (\log \log N)^{\frac{\ell}{2}} \\ \frac{\log \log N}{\log N} &\geq \frac{20\ell}{\epsilon^2} \end{aligned}$$

one can check that

$$\mathcal{E}_1(N, A, B, \ell) \ll O\left(\frac{1}{(\log N)^{\ell+\gamma_2}}\right).$$

Before we proceed with estimating Σ_2 as defined in (4.8), we give a proof of Lemma 3. Later we are going to use the same proof and the discussions above to give a bound on Σ_2 .

4.1 Proof of Lemma 3:

Let χ_i and χ'_i be Dirichlet characters modulo p_i for $1 \leq i \leq \ell$ and let χ_0 denote the principal character modulo n for any integer n . Let

$$\mathcal{A}(\chi) := \sum_{|a| \leq A} \chi(a) \quad \text{and} \quad \mathcal{B}(\chi) := \sum_{|b| \leq B} \chi(b).$$

For $U := (u_1, \dots, u_\ell) \in \mathbb{F}_{p_1}^* \times \dots \times \mathbb{F}_{p_\ell}^* = \mathbb{F}(P)^*$,

$$\begin{aligned} Z(P, S, T) &= \sum_{\substack{|a| \leq A, |b| \leq B \\ \exists U \in \mathbb{F}(P)^* \\ a \equiv s_i u_i^4 \pmod{p_i}, b \equiv t_i u_i^6 \pmod{p_i} \\ 1 \leq i \leq \ell}} 1 \\ &= \frac{1}{2^\ell} \sum_{\substack{|a| \leq A \\ |b| \leq B}} \sum_{U \in \mathbb{F}(P)^*} \prod_{i=1}^{\ell} \left(\frac{1}{\varphi(p_i)^2} \sum_{\chi_i \pmod{p_i}} \chi_i(s_i u_i^4) \overline{\chi_i}(a) \sum_{\chi'_i \pmod{p_i}} \chi'_i(t_i u_i^6) \overline{\chi'_i}(b) \right) \\ &= \frac{1}{2^\ell} \prod_{i=1}^{\ell} \frac{1}{(p_i - 1)^2} \sum_{U \in \mathbb{F}(P)^*} \sum_{\substack{\chi_i, \chi'_i \pmod{p_i} \\ 1 \leq i \leq \ell}} \chi_i(s_i) \chi'_i(t_i) \chi_i(u_i^4) \chi'_i(u_i^6) \sum_{\substack{|a| \leq A \\ |b| \leq B}} \overline{\chi_1 \cdots \chi_\ell}(a) \overline{\chi'_1 \cdots \chi'_\ell}(b). \end{aligned} \tag{4.15}$$

By the orthogonality relations of Dirichlet characters, we have

$$\prod_{i=1}^{\ell} \sum_{U \in \mathbb{F}_{p_i}^*} \chi_i(u_i^4) \chi'_i(u_i^6) = \begin{cases} \prod_{i=1}^{\ell} (p_i - 1) & \text{if } \chi_i^4 (\chi'_i)^6 = \chi_0 \pmod{p_i} \text{ for } 1 \leq i \leq \ell, \\ 0 & \text{otherwise.} \end{cases} \tag{4.16}$$

Then combining (4.15) and (4.16), we get

$$\begin{aligned}
 Z(P, S, T) &= \frac{1}{2^\ell} \sum_{\substack{\chi_1, \dots, \chi_\ell \\ \chi'_1, \dots, \chi'_\ell \\ \chi_i^4(\chi'_i)^6 = \chi_0 \pmod{p_i} \\ \text{for } 1 \leq i \leq \ell}} \prod_{i=1}^{\ell} \left(\frac{\chi_i(s_i) \chi'_i(t_i)}{p_i - 1} \right) \mathcal{A}(\overline{\chi_1 \cdots \chi_\ell}) \mathcal{B}(\overline{\chi'_1 \cdots \chi'_\ell}) \\
 &= \frac{1}{2^\ell} \left[\sum_{\substack{\chi_i = \chi'_i = \chi_0 \pmod{p_i} \\ \text{for } 1 \leq i \leq \ell}} + \sum_{\substack{\chi_i = (\chi'_i)^6 = \chi_0 \pmod{p_i} \\ \text{for } 1 \leq i \leq \ell \text{ and} \\ \exists 1 \leq j \leq \ell \text{ s.t. } \chi'_j \neq \chi_0 \pmod{p_j}}} + \sum_{\substack{\chi'_i = \chi_i^4 = \chi_0 \pmod{p_i} \\ \text{for } 1 \leq i \leq \ell \text{ and} \\ \exists 1 \leq j \leq \ell \text{ s.t. } \chi_j \neq \chi_0 \pmod{p_j}}} \right. \\
 &\quad \left. + \sum_{\substack{\chi_i^4(\chi'_i)^6 = \chi_0 \pmod{p_i} \\ \text{for } 1 \leq i \leq \ell \text{ and} \\ \exists 1 \leq r, s \leq \ell \text{ s.t. } \chi_r \neq \chi_0 \pmod{p_r}, \\ \chi'_s \neq \chi_0 \pmod{p_s}}} \right] \prod_{i=1}^{\ell} \left(\frac{\chi_i(s_i) \chi'_i(t_i)}{p_i - 1} \right) \mathcal{A}(\overline{\chi_1 \cdots \chi_\ell}) \mathcal{B}(\overline{\chi'_1 \cdots \chi'_\ell}) \\
 &= Z_1(P, S, T) + Z_2(P, S, T) + Z_3(P, S, T) + Z_4(P, S, T)
 \end{aligned} \tag{4.17}$$

Then, the LHS of (4.10), can be written as,

$$\begin{aligned}
 &\sum_{\substack{N^- < p_i < N^+ \\ 1 \leq i \leq \ell \\ pm \neq pn, \forall m \neq n}} \prod_{i=1}^{\ell} \frac{1}{p_i} \sum_{S, T \in \mathbb{F}(P)^*} h(P, N, S, T) \left(Z(P, S, T) - \frac{AB}{2^{\ell-2} p_1 \cdots p_\ell} \right) \\
 &= \sum_{\substack{N^- < p_i < N^+ \\ 1 \leq i \leq \ell \\ pm \neq pn, \forall m \neq n}} \prod_{i=1}^{\ell} \frac{1}{p_i} \sum_{S, T \in \mathbb{F}(P)^*} h(P, N, S, T) \left(\sum_{j=1}^4 Z_j(P, S, T) - \frac{AB}{2^{\ell-2} p_1 \cdots p_\ell} \right).
 \end{aligned} \tag{4.18}$$

Case 1: $\chi_i = \chi'_i = \chi_0 \pmod{p_i}$ for $1 \leq i \leq \ell$.

In this case,

$$\begin{aligned}
 \mathcal{A}(\overline{\chi_1 \cdots \chi_\ell}) &= \sum_{|a| \leq A} \chi_0(a) = \sum_{\substack{|a| \leq A \\ (a, p_1 \cdots p_\ell) = 1}} 1 = 2A \frac{\varphi(p_1 \cdots p_\ell)}{p_1 \cdots p_\ell} + O(\tau(p_1 \cdots p_\ell)) \\
 &= 2A \left(\frac{(p_1 - 1) \cdots (p_\ell - 1)}{p_1 \cdots p_\ell} \right) + O_\ell(1)
 \end{aligned} \tag{4.19}$$

and

$$\mathcal{B}(\overline{\chi'_1 \cdots \chi'_\ell}) = 2B \left(\frac{(p_1 - 1) \cdots (p_\ell - 1)}{p_1 \cdots p_\ell} \right) + O_\ell(1).$$

Consequently,

$$\begin{aligned}
 Z_1(P, S, T) &= \frac{1}{2^\ell} \prod_{j=1}^{\ell} \frac{1}{p_j - 1} \left(\frac{2A(p_1 - 1) \cdots (p_\ell - 1)}{p_1 \cdots p_\ell} + O_\ell(1) \right) \left(\frac{2B(p_1 - 1) \cdots (p_\ell - 1)}{p_1 \cdots p_\ell} + O_\ell(1) \right) \\
 &= \frac{AB}{2^{\ell-2} p_1 \cdots p_\ell} + O_\ell \left(\frac{AB}{N^{\ell+1}} + \frac{A + B + 1}{N^\ell} \right).
 \end{aligned} \tag{4.20}$$

Combining (4.12) with (4.20) and using Lemma 1, we get

$$\begin{aligned}
 & \sum_{\substack{N^- < p_i < N^+ \\ 1 \leq i \leq \ell \\ p_m \neq p_n, \forall m \neq n}} \prod_{i=1}^{\ell} \frac{1}{p_i} \sum_{S, T \in \mathbb{F}(P)^*} h(P, S, T) \left(Z_1(P, S, T) - \frac{AB}{2^{\ell-2} p_1 \cdots p_{\ell}} \right) \\
 & \ll_{\ell} \sum_{\substack{N^- < p_i < N^+ \\ 1 \leq i \leq \ell \\ p_m \neq p_n, \forall m \neq n}} \prod_{i=1}^{\ell} \frac{1}{p_i} \left(\frac{AB}{N^{\ell+1}} + \frac{A+B+1}{N^{\ell}} \right) \left(\prod_{j=1}^{\ell} (p_j - 1) H(D_N(p_j)) + N^{\frac{3\ell-1}{2}} (\log N)^{\ell-1} (\log \log N)^{\ell-1} \right) \\
 & \ll_{\ell} \frac{AB(\log \log N)}{N(\log N)^{\ell}} + \frac{(A+B+1)}{(\log N)^{\ell}}. \tag{4.21}
 \end{aligned}$$

Now,

$$\begin{aligned}
 Z_2(P, S, T) &= \frac{1}{2^{\ell}} \sum_{\substack{\chi_i = (\chi'_i)^6 = \chi_0 \pmod{p_i} \\ \text{for } 1 \leq i \leq \ell \text{ and} \\ \exists 1 \leq j \leq \ell \text{ s.t. } \chi'_j \neq \chi_0 \pmod{p_j}}} \prod_{i=1}^{\ell} \left(\frac{\chi_i(s_i) \chi'_i(t_i)}{p_i - 1} \right) \mathcal{A}(\overline{\chi_1 \cdots \chi_{\ell}}) \mathcal{B}(\overline{\chi'_1 \cdots \chi'_{\ell}}) \\
 &= \frac{1}{2^{\ell}} \sum_{\substack{(\chi'_i)^6 = \chi_0 \pmod{p_i} \\ \text{for } 1 \leq i \leq \ell \text{ and} \\ \exists 1 \leq j \leq \ell \text{ s.t. } \chi'_j \neq \chi_0 \pmod{p_j}}} \prod_{j=1}^{\ell} \frac{\chi'_j(t_j)}{(p_j - 1)} \left(2A \prod_{i=1}^{\ell} \frac{(p_i - 1)}{p_i} + O_{\ell}(1) \right) \mathcal{B}(\overline{\chi'_1 \cdots \chi'_{\ell}}) \\
 &\ll_{\ell} \frac{A}{p_1 \cdots p_{\ell}} \sum_{\substack{(\chi'_i)^6 = \chi_0 \pmod{p_i} \\ \text{for } 1 \leq i \leq \ell \text{ and} \\ \exists 1 \leq j \leq \ell \text{ s.t. } \chi'_j \neq \chi_0 \pmod{p_j}}} |\mathcal{B}(\overline{\chi'_1 \cdots \chi'_{\ell}})|.
 \end{aligned}$$

Using (4.11) and Hölder's inequality, we get

$$\begin{aligned}
 & \sum_{\substack{N^- < p_i < N^+ \\ 1 \leq i \leq \ell \\ p_m \neq p_n, \forall m \neq n}} \prod_{i=1}^{\ell} \frac{1}{p_i} \sum_{S, T \in \mathbb{F}(P)^*} h(P, N, S, T)(Z_2(P, S, T)) \\
 & \ll_{\ell} A \sum_{\substack{N^- < p_i < N^+ \\ 1 \leq i \leq \ell \\ p_m \neq p_n, \forall m \neq n}} \prod_{j=1}^{\ell} \frac{H(D_N(p_j))}{p_j} \sum_{\substack{(\chi'_i)^6 = \chi_0 \pmod{p_i} \\ \text{for } 1 \leq i \leq \ell \text{ and} \\ \exists 1 \leq j \leq \ell \text{ s.t. } \chi'_j \neq \chi_0 \pmod{p_j}}} |\mathcal{B}(\overline{\chi'_1 \cdots \chi'_\ell})| \\
 & \ll_{\ell} A \left(\sum_{\substack{N^- < p_i < N^+ \\ 1 \leq i \leq \ell \\ p_m \neq p_n, \forall m \neq n}} \sum_{\substack{(\chi'_i)^6 = \chi_0 \pmod{p_i} \\ \text{for } 1 \leq i \leq \ell \text{ and} \\ \exists 1 \leq j \leq \ell \text{ s.t. } \chi'_j \neq \chi_0 \pmod{p_j}}} \prod_{j=1}^{\ell} \left(\frac{H(D_N(p_j))}{p_j} \right)^{\frac{2k}{2k-1}} \right)^{1 - \frac{1}{2k}} \\
 & \quad \times \left(\sum_{\substack{N^- < p_i < N^+ \\ 1 \leq i \leq \ell \\ p_m \neq p_n, \forall m \neq n}} \sum_{\substack{(\chi'_i)^6 = \chi_0 \pmod{p_i} \\ \text{for } 1 \leq i \leq \ell \text{ and} \\ \exists 1 \leq j \leq \ell \text{ s.t. } \chi'_j \neq \chi_0 \pmod{p_j}}} |\mathcal{B}(\overline{\chi'_1 \cdots \chi'_\ell})|^{2k} \right)^{\frac{1}{2k}} \\
 & \ll_{\ell} A \left(\sum_{\substack{N^- < p_i < N^+ \\ p_i \neq p_j, \forall i \neq j \\ 1 \leq i \leq \ell}} \left(\frac{(\log p_i)^{\ell} (\log \log p_i)^{\ell}}{p_i^{\frac{\ell}{2}}} \right)^{\frac{2k}{2k-1}} \right)^{1 - \frac{1}{2k}} \\
 & \quad \times \left(\sum_{\substack{N^- < p_i < N^+ \\ 1 \leq i \leq \ell \\ p_m \neq p_n, \forall m \neq n}} \sum_{\substack{(\chi'_i)^6 = \chi_0 \pmod{p_i} \\ \text{for } 1 \leq i \leq \ell \text{ and} \\ \exists 1 \leq j \leq \ell \text{ s.t. } \chi'_j \neq \chi_0 \pmod{p_j}}} |\mathcal{B}(\overline{\chi'_1 \cdots \chi'_\ell})|^{2k} \right)^{\frac{1}{2k}} \\
 & \ll_{\ell} N^{-\frac{\ell}{4k}} (\log N)^{\frac{\ell}{2k}} (\log \log N)^{\ell} \left(\sum_{\substack{N^- < p_i < N^+ \\ 1 \leq i \leq \ell \\ p_m \neq p_n, \forall m \neq n}} \sum_{\substack{(\chi'_i)^6 = \chi_0 \pmod{p_i} \\ \text{for } 1 \leq i \leq \ell \text{ and} \\ \exists 1 \leq j \leq \ell \text{ s.t. } \chi'_j \neq \chi_0 \pmod{p_j}}} |\mathcal{B}(\overline{\chi'_1 \cdots \chi'_\ell})|^{2k} \right)^{\frac{1}{2k}}
 \end{aligned} \tag{4.22}$$

Now, for a fixed prime ℓ -tuple $(p_1, p_2, \dots, p_{\ell})$, the second product in (4.22), let $J \subseteq \{1, \dots, \ell\}$ be the set of positive integers such that $\chi'_j \neq \chi_0 \pmod{p_j}$ for $j \in J$. Thus,

$$|\mathcal{B}(\overline{\chi'_1 \cdots \chi'_\ell})| = \left| \sum_{|b| \leq B} \overline{\chi'_1}(b) \cdots \overline{\chi'_\ell}(b) \right| = \left| \sum_{|b| \leq B} \prod_{j \in J} \overline{\chi'_j}(b) \prod_{j \notin J} \overline{\chi'_j}(b) \right| = \left| \sum_{\substack{|b| \leq B \\ (b, \prod_{j \notin J} p_j) = 1}} \prod_{j \in J} \overline{\chi'_j}(b) \right|.$$

Let $\tau_k(b; B)$ denote the number of representation of b as a product of k positive B smooth

integers. Then,

$$\left| \sum_{\substack{|b| \leq B \\ (b, \prod_{j \in J} p_j) = 1}} \prod_{j \in J} \overline{\chi'_j(b)} \right|^{2k} \ll_\ell \left| \sum_{\substack{b \leq B^k \\ (b, \prod_{j \notin J} p_j) = 1}} \tau_k(b; B) \prod_{j \in J} \overline{\chi'_j(b)} \right|^2.$$

Thus,

$$\begin{aligned} & \left(\sum_{\substack{N^- < p_i < N^+ \\ 1 \leq i \leq \ell \\ p_m \neq p_n, \forall m \neq n}} \sum_{\substack{(\chi'_i)^6 = \chi_0 \pmod{p_i} \\ \text{for } 1 \leq i \leq \ell \text{ and} \\ \exists 1 \leq j \leq \ell \text{ s.t. } \chi'_j \neq \chi_0 \pmod{p_j}}} |\mathcal{B}(\overline{\chi'_1 \cdots \chi'_\ell})|^{2k} \right)^{\frac{1}{2k}} \\ & \ll_\ell \left(\sum_{\substack{N^- < p_i < N^+ \\ 1 \leq i \leq \ell \\ p_m \neq p_n, \forall m \neq n}} \sum_{\substack{(\chi'_i)^6 = \chi_0 \pmod{p_i} \\ \text{for } 1 \leq i \leq \ell \text{ and} \\ \exists 1 \leq j \leq \ell \text{ s.t. } \chi'_j \neq \chi_0 \pmod{p_j}}} \left| \sum_{\substack{b \leq B^k \\ (b, \prod_{j \notin J} p_j) = 1}} \tau_k(b; B) \prod_{j \in J} \overline{\chi'_j(b)} \right|^2 \right)^{\frac{1}{2k}}. \quad (4.23) \end{aligned}$$

Now, $(\overline{\prod_{j \in J} \chi'_j})(b)$ is a primitive character modulo $\prod_{j \in J} p_j \leq N^\ell$. Now we extend the sum in (4.23) to a sum over all primitive characters modulo d for all modulus $d \leq N^\ell$. Using Theorem 3, we get

$$\begin{aligned} & \left(\sum_{\substack{N^- < p_i < N^+ \\ 1 \leq i \leq \ell \\ p_m \neq p_n, \forall m \neq n}} \sum_{\substack{(\chi'_i)^6 = \chi_0 \pmod{p_i} \\ \text{for } 1 \leq i \leq \ell \text{ and} \\ \exists 1 \leq j \leq \ell \text{ s.t. } \chi'_j \neq \chi_0 \pmod{p_j}}} |\mathcal{B}(\overline{\chi'_1 \cdots \chi'_\ell})|^{2k} \right)^{\frac{1}{2k}} \ll_\ell \left(\sum_{\substack{d \leq N^\ell \\ \chi \pmod{d} \\ \chi \text{ primitive}}} \left| \sum_{b \leq B^k} \tau_k(b; B) \chi(b) \right|^2 \right)^{\frac{1}{2k}} \\ & \ll_\ell \left(\sum_{\substack{d \leq N^\ell \\ \chi \pmod{d} \\ \chi \text{ primitive}}} \left| \sum_{b \leq B^k} \tau_k(b) \chi(b) \right|^2 \right)^{\frac{1}{2k}} \\ & \ll_\ell \left((B^k + N^{2\ell}) \sum_{b \leq B^k} |\tau_k(b)|^2 \right)^{\frac{1}{2k}} \\ & \ll_\ell \left((B^k + N^{2\ell}) B^k \log^{k^2-1}(B^k) \right)^{\frac{1}{2k}} \quad (4.24) \end{aligned}$$

Combining (4.22) and (4.24), we get

$$\begin{aligned}
 & \sum_{\substack{N^- < p_i < N^+ \\ 1 \leq i \leq \ell \\ p_m \neq p_n, \forall m \neq n}} \prod_{i=1}^{\ell} \frac{1}{p_i} \sum_{S, T \in \mathbb{F}(P)^*} h(P, N, S, T) Z_2(P, S, T) \\
 & \ll_{\ell} A \sum_{\substack{N^- < p_i < N^+ \\ 1 \leq i \leq \ell \\ p_m \neq p_n, \forall m \neq n}} \prod_{i=1}^{\ell} \frac{1}{p_i} \prod_{j=1}^{\ell} H(D_N(p_j)) \sum_{\substack{(\chi'_i)^6 = \chi_0 \pmod{p_i} \\ \text{for } 1 \leq i \leq \ell \text{ and} \\ \exists 1 \leq j \leq \ell \text{ s.t. } \chi'_j \neq \chi_0 \pmod{p_j}}} |\mathcal{B}(\overline{\chi'_1 \cdots \chi'_\ell})| \\
 & \ll_{\ell} A \left((B^k + N^{2\ell}) B^k \log^{k^2-1}(B^k) \right)^{\frac{1}{2k}} N^{-\frac{\ell}{4k}} (\log N)^{\frac{\ell}{2k}} (\log \log N)^{\ell} \\
 & \ll_{\ell, k} A B N^{-\frac{\ell}{4k}} (\log N)^{\frac{\ell}{2k}} (\log \log N)^{\ell} \log^{\frac{k^2-1}{2k}} B + A \sqrt{B} N^{\frac{3\ell}{4k}} (\log N)^{\frac{k^2+\ell-1}{2k}} (\log \log N)^{\ell}.
 \end{aligned} \tag{4.25}$$

Following almost similar arguments,

$$Z_3(P, S, T) \ll_{\ell} \frac{B}{p_1 \cdots p_{\ell}} \sum_{\substack{\chi_i^4 = \chi_0 \pmod{p_i} \\ \text{for } 1 \leq i \leq \ell \text{ and} \\ \exists 1 \leq j \leq \ell \text{ s.t. } \chi_j \neq \chi_0 \pmod{p_j}}} |\mathcal{A}(\overline{\chi_1 \cdots \chi_{\ell}})|.$$

and

$$\begin{aligned}
 & \sum_{\substack{N^- < p_i < N^+ \\ 1 \leq i \leq \ell \\ p_m \neq p_n, \forall m \neq n}} \prod_{i=1}^{\ell} \frac{1}{p_i} \sum_{S, T \in \mathbb{F}(P)^*} h(P, N, S, T) Z_3(P, S, T) \\
 & \ll B \sum_{\substack{N^- < p_i < N^+ \\ 1 \leq i \leq \ell \\ p_m \neq p_n, \forall m \neq n}} \prod_{i=1}^{\ell} \frac{1}{p_i} \prod_{j=1}^{\ell} H(D_N(p_j)) \sum_{\substack{\chi_i^4 = \chi_0 \pmod{p_i} \\ \text{for } 1 \leq i \leq \ell \text{ and} \\ \exists 1 \leq j \leq \ell \text{ s.t. } \chi_j \neq \chi_0 \pmod{p_j}}} |\mathcal{A}(\overline{\chi_1 \cdots \chi_{\ell}})| \\
 & \ll_{\ell, k} A B N^{-\frac{\ell}{4k}} (\log N)^{\frac{\ell}{2k}} (\log \log N)^{\ell} \log^{\frac{k^2-1}{2k}} A + B \sqrt{A} N^{\frac{3\ell}{4k}} (\log N)^{\frac{k^2+\ell-1}{2k}} (\log \log N)^{\ell}
 \end{aligned} \tag{4.26}$$

for a positive real number $k > \frac{1}{2}$. Hence,

$$\begin{aligned}
 & \sum_{\substack{N^- < p_i < N^+ \\ 1 \leq i \leq \ell \\ p_m \neq p_n, \forall m \neq n}} \prod_{i=1}^{\ell} \frac{1}{p_i} \sum_{S, T \in \mathbb{F}(P)^*} h(P, N, S, T) (Z_2(P, S, T) + Z_3(P, S, T)) \\
 & \ll_{k, \ell} A B N^{-\frac{\ell}{4k}} (\log N)^{\frac{\ell}{2k}} (\log \log N)^{\ell} (\log^{\frac{k^2-1}{2k}} A + \log^{\frac{k^2-1}{2k}} B) + (A \sqrt{B} + B \sqrt{A}) N^{\frac{3\ell}{4k}} (\log N)^{\frac{k^2+\ell}{2k}} (\log \log N)^{\ell}
 \end{aligned} \tag{4.27}$$

Finally, for $Z_4(P, S, T)$, define

$$g(P, \chi_i, \chi'_i) := \sum_{\substack{1 \leq s_i, t_i < p_i \\ 1 \leq i \leq \ell}} h(P, N, S, T) \chi_i(s_i) \chi'_i(t_i).$$

Then,

$$\begin{aligned}
 & \sum_{\substack{N^- < p_i < N^+ \\ 1 \leq i \leq \ell \\ pm \neq pn, \forall m \neq n}} \prod_{i=1}^{\ell} \frac{1}{p_i} \sum_{S, T \in \mathbb{F}(P)^*} h(P, N, S, T) Z_4(P, S, T) \\
 &= \frac{1}{2^\ell} \sum_{\substack{N^- < p_i < N^+ \\ 1 \leq i \leq \ell \\ pm \neq pn, \forall m \neq n}} \prod_{j=1}^{\ell} \frac{1}{p_j(p_j - 1)} \sum_{\substack{\chi_i^4(\chi'_i)^6 = \chi_0 \pmod{p_i} \\ \text{for } 1 \leq i \leq \ell \text{ and} \\ \exists 1 \leq r, s \leq \ell \text{ s.t. } \chi_r \neq \chi_0 \pmod{p_r}, \\ \chi'_s \neq \chi_0 \pmod{p_s}}} g(P, \chi_i, \chi'_i) \mathcal{A}(\overline{\chi_1 \cdots \chi_\ell}) \mathcal{B}(\overline{\chi'_1 \cdots \chi'_\ell}).
 \end{aligned} \tag{4.28}$$

Applying Hölder's inequality again, we have

$$\begin{aligned}
 & \left| \sum_{\substack{\chi_i^4(\chi'_i)^6 = \chi_0 \pmod{p_i} \\ \text{for } 1 \leq i \leq \ell \text{ and} \\ \exists 1 \leq r, s \leq \ell \text{ s.t. } \chi_r \neq \chi_0 \pmod{p_r}, \\ \chi'_s \neq \chi_0 \pmod{p_s}}} g(P, \chi_i, \chi'_i) \mathcal{A}(\overline{\chi_1 \cdots \chi_\ell}) \mathcal{B}(\overline{\chi'_1 \cdots \chi'_\ell}) \right| \\
 & \leq \left| \sum_{\substack{\chi_i^4(\chi'_i)^6 = \chi_0 \pmod{p_i} \\ \text{for } 1 \leq i \leq \ell \text{ and} \\ \exists 1 \leq r, s \leq \ell \text{ s.t. } \chi_r \neq \chi_0 \pmod{p_r}, \\ \chi'_s \neq \chi_0 \pmod{p_s}}} |g(P, \chi_i, \chi'_i)|^2 \right|^{\frac{1}{2}} \left(\sum_{\substack{\chi_i^4(\chi'_i)^6 = \chi_0 \pmod{p_i} \\ \text{for } 1 \leq i \leq \ell \text{ and} \\ \exists 1 \leq r, s \leq \ell \text{ s.t. } \chi_r \neq \chi_0 \pmod{p_r}, \\ \chi'_s \neq \chi_0 \pmod{p_s}}} |\mathcal{A}(\overline{\chi_1 \cdots \chi_\ell})|^4 \right)^{\frac{1}{4}} \\
 & \times \left(\sum_{\substack{\chi_i^4(\chi'_i)^6 = \chi_0 \pmod{p_i} \\ \text{for } 1 \leq i \leq \ell \text{ and} \\ \exists 1 \leq r, s \leq \ell \text{ s.t. } \chi_r \neq \chi_0 \pmod{p_r}, \\ \chi'_s \neq \chi_0 \pmod{p_s}}} |\mathcal{B}(\overline{\chi'_1 \cdots \chi'_\ell})|^4 \right)^{\frac{1}{4}}.
 \end{aligned} \tag{4.29}$$

Now, extending the sum over all non-principal characters modulo N^ℓ , from Theorem 4 we have

$$\begin{aligned}
 & \sum_{\substack{\chi_i^4(\chi'_i)^6 = \chi_0 \pmod{p_i} \\ \text{for } 1 \leq i \leq \ell \text{ and} \\ \exists 1 \leq r, s \leq \ell \text{ s.t. } \chi_r \neq \chi_0 \pmod{p_r}, \\ \chi'_s \neq \chi_0 \pmod{p_s}}} |\mathcal{A}(\overline{\chi_1 \cdots \chi_\ell})|^4 \ll_\ell \sum_{\chi \neq \chi_0 \pmod{N^\ell}} \left| \sum_{|a| \leq A} \overline{\chi}(a) \right|^4 \\
 & \ll_\ell A^2 N^\ell (\log(N^\ell))^6 \ll_\ell A^2 N^\ell (\log N)^6
 \end{aligned} \tag{4.30}$$

Similarly,

$$\begin{aligned}
 & \sum_{\substack{\chi_i^4(\chi'_i)^6 = \chi_0 \pmod{p_i} \\ \text{for } 1 \leq i \leq \ell \text{ and} \\ \exists 1 \leq r, s \leq \ell \text{ s.t. } \chi_r \neq \chi_0 \pmod{p_r}, \\ \chi'_s \neq \chi_0 \pmod{p_s}}} |\mathcal{B}(\overline{\chi'_1 \cdots \chi'_\ell})|^4 \ll_\ell \left(\sum_{\chi' \neq \chi_0 \pmod{N^\ell}} \left| \sum_{|b| \leq B} \overline{\chi'}(b) \right|^4 \right) \\
 & \ll_\ell B^2 N^\ell (\log(N^\ell))^6 \ll_\ell B^2 N^\ell (\log N)^6
 \end{aligned} \tag{4.31}$$

Further, from (4.29), we have

$$\begin{aligned}
 & \sum_{\substack{\chi_i^4(\chi'_i)^6 = \chi_0 \pmod{p_i} \\ \text{for } 1 \leq i \leq \ell \text{ and} \\ \exists 1 \leq r, s \leq \ell \text{ s.t. } \chi_r \neq \chi_0 \pmod{p_r}, \\ \chi'_s \neq \chi_0 \pmod{p_s}}} |g(P, \chi_i, \chi'_i)|^2 \leq \sum_{\substack{\chi_i, \chi'_i \pmod{p_i} \\ 1 \leq i \leq \ell}} |g(P, \chi_i, \chi'_i)|^2 \\
 & \leq \sum_{S, T \in \mathbb{F}(P)^*} \sum_{S', T' \in \mathbb{F}(P)^*} h(P, N, S, T) \overline{h(P, N, S', T')} \sum_{\chi_i \pmod{p_i}} \chi_i(s_i) \overline{\chi_i(s'_i)} \sum_{\chi'_i \pmod{p_i}} \chi'_i(t_i) \overline{\chi'_i(t'_i)} \\
 & = \prod_{i=1}^{\ell} (p_i - 1)^2 \sum_{S, T \in \mathbb{F}(P)^*} |h(P, N, S, T)| \\
 & = \prod_{i=1}^{\ell} (p_i - 1)^2 \sum_{S, T \in \mathbb{F}(P)^*} |h(P, N, S, T)|^2 \\
 & = N^{3\ell} \prod_{i=1}^{\ell} H(D_N(p_i)) + O_{\ell} \left(N^{\frac{7\ell-1}{2}} (\log N)^{\ell} (\log \log N)^{\ell} \right), \tag{4.32}
 \end{aligned}$$

Combining (4.29), (4.30), (4.31) and (4.32), we have

$$\begin{aligned}
 & \left| \sum_{\substack{\chi_i^4(\chi'_i)^6 = \chi_0 \pmod{p_i} \\ \text{for } 1 \leq i \leq \ell \text{ and} \\ \exists 1 \leq r, s \leq \ell \text{ s.t. } \chi_r \neq \chi_0 \pmod{p_r}, \\ \chi'_s \neq \chi_0 \pmod{p_s}}} g(P, \chi_i, \chi'_i) \mathcal{A}(\overline{\chi_1 \cdots \chi_{\ell}}) \mathcal{B}(\overline{\chi'_1 \cdots \chi'_{\ell}}) \right| \\
 & \ll_{\ell} \sqrt{AB} N^{2\ell} (\log N)^3 \prod_{i=1}^{\ell} (H(D_N(p_i)))^2 \tag{4.33}
 \end{aligned}$$

Thus (4.33) and (4.28) gives

$$\begin{aligned}
 & \sum_{\substack{N^- < p_i < N^+ \\ 1 \leq i \leq \ell \\ p_m \neq p_n, \forall m \neq n}} \prod_{i=1}^{\ell} \frac{1}{p_i} \sum_{S, T \in \mathbb{F}(P)^*} h(P, N, S, T) Z_4(P, S, T) \\
 & \ll_{\ell} \sqrt{AB} (\log N)^3 \sum_{\substack{N^- < p_i < N^+ \\ 1 \leq i \leq \ell \\ p_m \neq p_n, \forall m \neq n}} \prod_{i=1}^{\ell} \sqrt{H(D_N(p_j))} \tag{4.34}
 \end{aligned}$$

Using Lemma 1 and Cauchy-Schwarz inequality, we get

$$\begin{aligned}
 & \sum_{\substack{N^- < p_i < N^+ \\ 1 \leq i \leq \ell \\ p_m \neq p_n, \forall m \neq n}} \prod_{i=1}^{\ell} \sqrt{H(D_N(p_j))} \ll_{\ell} \left(\sum_{\substack{N^- < p_i < N^+ \\ 1 \leq i \leq \ell \\ p_m \neq p_n, \forall m \neq n}} \prod_{i=1}^{\ell} H(D_N(p_i)) \right)^{\frac{1}{2}} \left(\sum_{\substack{N^- < p_i < N^+ \\ 1 \leq i \leq \ell \\ p_m \neq p_n, \forall m \neq n}} 1 \right)^{\frac{1}{2}} \\
 & \ll_{\ell} \frac{N^{\frac{3\ell}{4}} (\log \log N)^{\frac{\ell}{2}}}{(\log N)^{\ell}} \tag{4.35}
 \end{aligned}$$

Thus,

$$\sum_{\substack{N^- < p_i < N^+ \\ 1 \leq i \leq \ell \\ p_m \neq p_n, \forall m \neq n}} \prod_{i=1}^{\ell} \frac{1}{p_i} \sum_{S, T \in \mathbb{F}(P)^*} h(P, N, S, T) Z_4(P, S, T) \ll_{\ell} \sqrt{AB} N^{\frac{3\ell}{4}} (\log N)^{3-\ell} (\log \log N)^{\frac{\ell}{2}} \quad (4.36)$$

Finally, combining (4.21), (4.27) and (4.36), we complete the proof of Lemma 3.

4.2 Bound on Σ_2 :

Next, we plan to modify the previous proof of Lemma 3 to give an upper bound on Σ_2 . Recall,

$$\Sigma_2 = \frac{1}{\#\mathcal{C}(A, B)} \sum_{\substack{N^- < p_i < N^+ \\ 1 \leq i \leq \ell \\ p_m \neq p_n, \forall m \neq n}} \sum_{\substack{S, T \in \mathbb{F}(P) \\ s_i t_i = 0 \text{ for some } i \\ 1 \leq i \leq \ell}} h(P, N, S, T) Z(P, S, T) \prod_{j=1}^{\ell} \frac{\# \text{Aut}(E_{p_j, s_j, t_j})}{p_j - 1} \quad (4.37)$$

Case 1: $s_i t_i = 0$ for all i .

Then the corresponding rational curves look like $E_{a,b}$ where $p_1 p_2 \cdots p_{\ell} \mid a$ or $p_1 p_2 \cdots p_{\ell} \mid b$. In that case, the contribution corresponding to $ab \neq 0$ is bounded by

$$\frac{1}{4AB} \sum_{\substack{N^- < p_i < N^+ \\ 1 \leq i \leq \ell \\ p_m \neq p_n, \forall m \neq n}} \frac{AB}{p_1 p_2 \cdots p_{\ell}} \ll_{\ell} N^{-\frac{\ell}{2}} \quad (4.38)$$

If, either $a = 0$ or $b = 0$, then the curve has complex multiplication. Hence, by Kowalski [Kow06], there are only $O_{\epsilon, \ell}(N^{\frac{\epsilon}{2\ell}})$ many primes such that $\#E_p(\mathbb{F}_p) = N$. So, the contribution corresponding to $ab = 0$ is bounded by

$$O_{\epsilon, \ell} \left(\frac{N^{\frac{\epsilon}{2}}(A+B)}{AB} \right) = O_{\epsilon, \ell} \left(N^{\frac{\epsilon}{2}} \left(\frac{1}{A} + \frac{1}{B} \right) \right) \quad (4.39)$$

Case 2: $s_{j_1} s_{j_1} \neq 0$ for some j_1 and $s_{j_2} s_{j_2} = 0$ for some j_2 .

The number of possible subsets I of $\{1, 2, \dots, \ell\}$ such that $s_i t_i = 0$ for all $i \in I$ is bounded by $O_{\ell}(1)$. Take one such subset I and without loss of generality, assume that $\#I = e + f$ with

$$s_1 = s_2 = \cdots = s_e = 0, \quad t_{e+1} = t_{e+2} = \cdots = t_{e+f} = 0, \quad \text{and } s_i t_i \neq 0 \text{ for } e+f+1 \leq i \leq \ell.$$

In that case, the contribution corresponding to the set I in (4.37) is bounded by

$$\frac{1}{4AB} \left(\sum_{\substack{N^- < p_i < N^+ \\ 1 \leq i \leq e+f \\ p_m \neq p_n, \forall m \neq n}} \prod_{i=1}^{e+f} \frac{1}{(p_i - 1)} \right) \sum_{\substack{N^- < p_i < N^+ \\ e+f+1 \leq i \leq \ell \\ p_m \neq p_n, \forall m \neq n}} \prod_{i=e+f+1}^{\ell} \frac{1}{p_i - 1} \sum_{\hat{S}, \hat{T} \in \mathbb{F}(\hat{P})^*} \hat{h}(\hat{P}, N, \hat{S}, \hat{T}) \hat{Z}(\hat{P}, \hat{S}, \hat{T}) \quad (4.40)$$

where

$$\begin{aligned}\hat{P} &:= (p_{e+f+1}, p_{e+f+2}, \dots, p_\ell) \\ \hat{S} &:= (s_{e+f+1}, s_{e+f+2}, \dots, s_\ell) \\ \hat{T} &:= (t_{e+f+1}, t_{e+f+2}, \dots, t_\ell) \\ \hat{h}(\hat{P}, N, \hat{S}, \hat{T}) &:= \begin{cases} 1 & \text{if } \#E_{p_i, s_i, t_i}(\mathbb{F}_{p_i}) = N \text{ for } e+f+1 \leq i \leq \ell, \\ 0 & \text{otherwise.} \end{cases}\end{aligned}$$

$$\begin{aligned}\hat{Z}(\hat{P}, \hat{S}, \hat{T}) &:= \sum_{\substack{|p_1 \cdots p_e a| \leq A, \\ |p_{e+1} \cdots p_{e+f} b| \leq B \\ p_1 \cdots p_e a \equiv s_i u_i^4 \pmod{p_i} \\ p_{e+1} \cdots p_{e+f} b \equiv t_i u_i^6 \pmod{p_i} \\ \text{for some } (u_{e+f+1}, \dots, u_\ell) \in \mathbb{F}(\hat{P})^*}} 1 \\ &= \frac{1}{2^\ell} \sum_{\substack{|a| \leq A/p_1 \cdots p_e \\ |b| \leq B/p_{e+1} \cdots p_{e+f}}} \sum_{\hat{U} \in \mathbb{F}(\hat{P})^*} \prod_{i=e+f+1}^{\ell} \\ &\quad \left(\frac{1}{\varphi(p_i)^2} \sum_{\chi_i \pmod{p_i}} \chi_i(s_i u_i^4) \overline{\chi_i}(p_1 \cdots p_e a) \sum_{\chi'_i \pmod{p_i}} \chi'_i(t_i u_i^6) \overline{\chi'_i}(p_{e+1} \cdots p_{e+f} b) \right)\end{aligned}$$

Then, (4.40) is bounded by

$$\frac{1}{4AB} \sum_{\substack{N^- < p_i < N^+ \\ 1 \leq i \leq e+f \\ p_m \neq p_n, \forall m \neq n}} \left(\prod_{i=1}^{e+f} \frac{1}{p_i - 1} \right) \hat{\mathcal{E}}_1(N, A, B, e+f+1, \ell) = O\left(\frac{\hat{\mathcal{E}}_1(N, A, B, e+f+1, \ell)}{ABN^{\frac{e+f}{2}}} \right) \quad (4.41)$$

where

$$\hat{\mathcal{E}}_1(N, A, B, e+f+1, \ell) = \sum_{\substack{N^- < p_i < N^+ \\ e+f+1 \leq i \leq \ell \\ p_m \neq p_n, \forall m \neq n}} \prod_{i=e+f+1}^{\ell} \frac{1}{p_i - 1} \sum_{\hat{S}, \hat{T} \in \mathbb{F}(\hat{P})^*} \hat{h}(\hat{P}, N, \hat{S}, \hat{T}) \hat{Z}(\hat{P}, \hat{S}, \hat{T})$$

We proceed with a argument almost similar to the proof of Lemma 3 to estimate

$$\begin{aligned}
 \hat{\mathcal{E}}_1(N, A, B, e+f+1, \ell) &= \sum_{\substack{N^- < p_i < N^+ \\ e+f+1 \leq i \leq \ell \\ p_m \neq p_n, \forall m \neq n}} \left(\prod_{i=e+f+1}^{\ell} \frac{1}{p_i - 1} \right) \sum_{\hat{S}, \hat{T} \in \mathbb{F}(\hat{P})^*} \hat{h}(\hat{P}, N, \hat{S}, \hat{T}) \hat{Z}(\hat{P}, \hat{S}, \hat{T}) \\
 &= \sum_{\substack{N^- < p_i < N^+ \\ e+f+1 \leq i \leq \ell \\ p_m \neq p_n, \forall m \neq n}} \left(\prod_{i=e+f+1}^{\ell} \frac{1}{p_i - 1} \right) \sum_{\hat{S}, \hat{T} \in \mathbb{F}(\hat{P})^*} \hat{h}(\hat{P}, N, \hat{S}, \hat{T}) \frac{AB/p_1 p_2 \cdots p_{e+f}}{2^{\ell-e-f-2} p_{e+f+1} \cdots p_{\ell}} \\
 &\quad + \sum_{\substack{N^- < p_i < N^+ \\ e+f+1 \leq i \leq \ell \\ p_m \neq p_n, \forall m \neq n}} \left(\prod_{i=e+f+1}^{\ell} \frac{1}{p_i - 1} \right) \sum_{\hat{S}, \hat{T} \in \mathbb{F}(\hat{P})^*} \hat{h}(\hat{P}, N, \hat{S}, \hat{T}) \left(\hat{Z}(\hat{P}, \hat{S}, \hat{T}) - \frac{AB/p_1 p_2 \cdots p_{e+f}}{2^{\ell-e-f-2} p_{e+f+1} \cdots p_{\ell}} \right)
 \end{aligned} \tag{4.42}$$

Define $\hat{\mathcal{A}}(\overline{\chi_{e+f+1} \cdots \chi_{\ell}})$ and $\hat{\mathcal{B}}(\overline{\chi'_{e+f+1} \cdots \chi'_{\ell}})$, by

$$\begin{aligned}
 \hat{\mathcal{A}}(\overline{\chi_{e+f+1} \cdots \chi_{\ell}}) &= \sum_{|a| \leq A/p_1 \cdots p_e} \overline{\chi_{e+f+1} \cdots \chi_{\ell}}(p_1, p_2 \cdots p_e a) \\
 &= \overline{\chi_{e+f+1} \cdots \chi_{\ell}}(p_1, \cdots p_e) \sum_{|a| \leq A/p_1 \cdots p_e} \overline{\chi_{e+f+1} \cdots \chi_{\ell}}(a) \\
 \hat{\mathcal{B}}(\overline{\chi'_{e+f+1} \cdots \chi'_{\ell}}) &= \sum_{|b| \leq B/p_{e+1} \cdots p_{e+f}} \overline{\chi'_{e+f+1} \cdots \chi'_{\ell}}(p_{e+1}, \cdots p_{e+f} b) \\
 &= \overline{\chi'_{e+f+1} \cdots \chi'_{\ell}}(p_{e+1}, \cdots p_{e+f}) \sum_{|b| \leq B/p_{e+1} \cdots p_{e+f}} \overline{\chi'_{e+f+1} \cdots \chi'_{\ell}}(b)
 \end{aligned}$$

First of all, using (4.11), note that the first summation on the right hand side of (4.42) is bounded by

$$O_{\ell} \left(AB N^{-e-f} \left(\sum_{N^- < p < N^+} \frac{H(D_N(p))}{p} \right)^{\ell-e-f} \right) = O_{\ell} \left(\frac{AB}{N^{e+f}} \left(\frac{\log \log N}{\log N} \right)^{\ell-e-f} \right)$$

Again, we write $\hat{Z}(\hat{P}, \hat{S}, \hat{T})$ as

$$\hat{Z}(\hat{P}, \hat{S}, \hat{T}) = \sum_{j=1}^4 \hat{Z}_j(\hat{P}, \hat{S}, \hat{T})$$

where

$$\begin{aligned}
 \hat{Z}_1(\hat{P}, \hat{S}, \hat{T}) &= \frac{1}{2^\ell} \sum_{\substack{\chi_i = \chi'_i = \chi_0 \pmod{p_i} \\ \text{for } 1 \leq i \leq \ell}} \prod_{i=e+f+1}^{\ell} \left(\frac{\chi_i(s_i) \chi'_i(t_i)}{p_i - 1} \right) \hat{\mathcal{A}}(\overline{\chi_{e+f+1} \cdots \chi_\ell}) \hat{\mathcal{B}}(\overline{\chi'_{e+f+1} \cdots \chi'_\ell}) \\
 \hat{Z}_2(\hat{P}, \hat{S}, \hat{T}) &= \frac{1}{2^\ell} \sum_{\substack{\chi_i = (\chi'_i)^6 = \chi_0 \pmod{p_i} \\ \text{for } 1 \leq i \leq \ell \text{ and} \\ \exists 1 \leq j \leq \ell \text{ s.t. } \chi'_j \neq \chi_0 \pmod{p_j}}} \prod_{i=e+f+1}^{\ell} \left(\frac{\chi_i(s_i) \chi'_i(t_i)}{p_i - 1} \right) \hat{\mathcal{A}}(\overline{\chi_{e+f+1} \cdots \chi_\ell}) \hat{\mathcal{B}}(\overline{\chi'_{e+f+1} \cdots \chi'_\ell}) \\
 \hat{Z}_3(\hat{P}, \hat{S}, \hat{T}) &= \frac{1}{2^\ell} \sum_{\substack{\chi'_i = \chi_i^4 = \chi_0 \pmod{p_i} \\ \text{for } 1 \leq i \leq \ell \text{ and} \\ \exists 1 \leq j \leq \ell \text{ s.t. } \chi_j \neq \chi_0 \pmod{p_j}}} \prod_{i=e+f+1}^{\ell} \left(\frac{\chi_i(s_i) \chi'_i(t_i)}{p_i - 1} \right) \hat{\mathcal{A}}(\overline{\chi_{e+f+1} \cdots \chi_\ell}) \hat{\mathcal{B}}(\overline{\chi'_{e+f+1} \cdots \chi'_\ell}) \\
 \hat{Z}_4(\hat{P}, \hat{S}, \hat{T}) &= \frac{1}{2^\ell} \sum_{\substack{\chi_i^4 (\chi'_i)^6 = \chi_0 \pmod{p_i} \\ \text{for } 1 \leq i \leq \ell \text{ and} \\ \exists 1 \leq r, s \leq \ell \text{ s.t. } \chi_r \neq \chi_0 \pmod{p_r}, \\ \chi'_s \neq \chi_0 \pmod{p_s}}} \prod_{i=e+f+1}^{\ell} \left(\frac{\chi_i(s_i) \chi'_i(t_i)}{p_i - 1} \right) \hat{\mathcal{A}}(\overline{\chi_{e+f+1} \cdots \chi_\ell}) \hat{\mathcal{B}}(\overline{\chi'_{e+f+1} \cdots \chi'_\ell})
 \end{aligned}$$

Now, let us denote $\hat{A} = \frac{A}{p_1 \cdots p_e}$ and $\hat{B} = \frac{B}{p_{e+1} \cdots p_{e+f}}$.

Then, following the same argument as the one we used to prove (4.21), we should get

$$\begin{aligned}
 &\sum_{\substack{N^- < p_i < N^+ \\ e+f+1 \leq i \leq \ell \\ p_m \neq p_n, \forall m \neq n}} \left(\prod_{i=e+f+1}^{\ell} \frac{1}{p_i - 1} \right) \sum_{\hat{S}, \hat{T} \in \mathbb{F}(\hat{P})^*} \hat{h}(\hat{P}, N, \hat{S}, \hat{T}) \left(\hat{Z}_1(\hat{P}, \hat{S}, \hat{T}) - \frac{AB/p_1 p_2 \cdots p_{e+f}}{2^{\ell-e-f-2} p_{e+f+1} \cdots p_\ell} \right) \\
 &\ll_\ell \frac{\hat{A} \hat{B} (\log \log N)}{N (\log N)^{\ell-e-f}} + \frac{(\hat{A} + \hat{B} + 1)}{(\log N)^{\ell-e-f}}
 \end{aligned} \tag{4.43}$$

Since, the primes p_i 's are distinct, we also have

$$\begin{aligned}
 |\overline{\chi_{m+n+1} \cdots \chi_\ell}(p_1, \cdots p_m)| &= 1 \\
 |\overline{\chi'_{m+n+1} \cdots \chi'_\ell}(p_{m+1}, \cdots p_{m+n})| &= 1,
 \end{aligned} \tag{4.44}$$

Hence,

$$\begin{aligned}
 \hat{Z}_2(\hat{P}, \hat{S}, \hat{T}) &\ll_\ell \frac{\hat{A}}{p_{e+f+1} \cdots p_\ell} \sum_{\substack{(\chi'_i)^6 = \chi_0 \pmod{p_i} \\ \text{for } e+f+1 \leq i \leq \ell \text{ and} \\ \exists e+f+1 \leq j \leq \ell \text{ s.t. } \chi'_j \neq \chi_0 \pmod{p_j}}} |\hat{\mathcal{B}}(\overline{\chi'_{e+f+1} \cdots \chi'_\ell})| \\
 &\ll_\ell \frac{A}{N^\ell} \sum_{\substack{(\chi'_i)^6 = \chi_0 \pmod{p_i} \\ \text{for } e+f+1 \leq i \leq \ell \text{ and} \\ \exists e+f+1 \leq j \leq \ell \text{ s.t. } \chi'_j \neq \chi_0 \pmod{p_j}}} \left| \sum_{|b| \leq B/p_{e+1} \cdots p_{e+f}} \overline{\chi'_{e+f+1} \cdots \chi'_\ell}(b) \right|
 \end{aligned}$$

and

$$\hat{Z}_3(\hat{P}, \hat{S}, \hat{T}) \ll_{\ell} \frac{B}{N^{\ell}} \sum_{\substack{\chi_i^4 = \chi_0 \pmod{p_i} \\ \text{for } e+f+1 \leq i \leq \ell \text{ and} \\ \exists e+f+1 \leq j \leq \ell \text{ s.t. } \chi_j \neq \chi_0 \pmod{p_j}}} \left| \sum_{|a| \leq A/p_1 \cdots p_e} \overline{\chi_{e+f+1} \cdots \chi_{\ell}}(a) \right|$$

Replacing A , B and ℓ by \hat{A} , \hat{B} and $\ell - e - f$ respectively in the proof of (4.27), we get the following inequality

$$\begin{aligned} & \sum_{\substack{N^- < p_i < N^+ \\ e+f+1 \leq i \leq \ell \\ p_m \neq p_n, \forall m \neq n}} \left(\prod_{i=e+f+1}^{\ell} \frac{1}{p_i - 1} \right) \sum_{\hat{S}, \hat{T} \in \mathbb{F}(\hat{P})^*} \hat{h}(\hat{P}, N, \hat{S}, \hat{T}) \left(\hat{Z}_2(\hat{P}, \hat{S}, \hat{T}) + \hat{Z}_3(\hat{P}, \hat{S}, \hat{T}) \right) \\ & \ll_{k, \ell} \hat{A} \hat{B} N^{-\frac{\ell-e-f}{4k}} (\log N)^{\frac{\ell-e-f}{2k}} (\log \log N)^{\ell-e-f} (\log^{\frac{k^2-1}{2k}} \hat{A} + \log^{\frac{k^2-1}{2k}} \hat{B}) \\ & \quad + (\hat{A} \sqrt{\hat{B}} + \hat{B} \sqrt{\hat{A}}) N^{\frac{3(\ell-e-f)}{4k}} (\log N)^{\frac{k^2+\ell-e-f}{2k}} (\log \log N)^{\ell-e-f} \end{aligned} \quad (4.45)$$

for some $k > \frac{1}{2}$.

Again, using (4.44) and replacing A , B and ℓ by \hat{A} , \hat{B} and $\ell - e - f$ respectively in the proof of (4.36), we get

$$\begin{aligned} & \sum_{\substack{N^- < p_i < N^+ \\ e+f+1 \leq i \leq \ell \\ p_m \neq p_n, \forall m \neq n}} \left(\prod_{i=e+f+1}^{\ell} \frac{1}{p_i - 1} \right) \sum_{\hat{S}, \hat{T} \in \mathbb{F}(\hat{P})^*} \hat{h}(\hat{P}, N, \hat{S}, \hat{T}) \hat{Z}_4(\hat{P}, \hat{S}, \hat{T}) \\ & \ll \sqrt{\hat{A} \hat{B}} N^{\frac{3(\ell-e-f)}{4}} (\log N)^{3-(\ell-e-f)} (\log \log N)^{\frac{\ell-e-f}{2}} \end{aligned} \quad (4.46)$$

Since $e + f \geq 1$, observe that we get a savings of a factor of $\frac{1}{\sqrt{N}}$ in (4.43), (4.45) and (4.46) compared to the upper bounds for corresponding expressions in the proof of Lemma 3. Also, in view of (4.39), we need to assume $A, B \geq N^{\epsilon}$ to make the corresponding error term sufficiently small in Proposition 1.

As a conclusion, it is safe to claim that Σ_2 is small enough compared to the the error term in Proposition 1. This completes the proof of Proposition 1. \square

REFERENCES

- AF15 A. Akbary and A. T. Felix, On invariants of elliptic curves on average. *Acta Arith.* **168** (2015), no. 1, 31-70.
- BG14 R. Balasubramanian and S. Giri, The mean-value of a product of shifted multiplicative functions and the average number of points of elliptic curves. *J. Number Theory* **157** (2015), 37-53.
- BG15 R. Balasubramanian and S. Giri, Poisson Distribution of a Prime Counting Function Corresponding to Elliptic Curves, to appear in *Internat. Math. Res. Notices*, arXiv:1503.01018 [math.NT].
- BCD11 A. Balog, A.-C. Cojocaru and C. David, Average twin prime conjecture for elliptic curves, *Amer. J. Math.* **133** (2011), no. 5, 1179-1229.
- BS09 W. D. Banks and I. E. Shparlinski, Sato-Tate, cyclicity, and divisibility statistics on average for elliptic curves of small height. *Israel J. Math.* **173** (2009), 253-277.

- CDKS14 V. Chandee, C. David, D. Koukoulopoulos and E. Smith, The Frequency of Elliptic Curve Groups Over Prime Finite Fields. *Canad. J. Math.* **68** (2016), no. 4, 721-761.
- Dav00 H. Davenport, Multiplicative number theory. Third edition. Revised and with a preface by Hugh L. Montgomery. Graduate Texts in Mathematics, 74. Springer-Verlag, New York, 2000.
- DS13 C. David and E. Smith, Elliptic curves with a given number of points over finite fields, *Compositio Math.* **149** (2013), 175203.
- DS14 C. David and E. Smith, Corrigendum to Elliptic curves with a given number of points over finite fields, *Compositio Math.* **150** (2014), no. 8, 13471348.
- Deu41 M. Deuring, Die Typen der Multiplikatorenringe elliptischer Funktionenkorpr. Abh. Math. Sem. Univ. Humbury, **14** (1941), no. 1, 197-272.
- FM96 E. Fouvry and M. R. Murty, On the distribution of supersingular primes, *Canad. J. Math.* **48** (1996), 81104.
- FI2 J. Friedlander and H. Iwaniec, The divisor problem for arithmetic progressions. *Acta Arith.* **45** (1985), 273-277.
- IK H. Iwaniec and E. Kowalski, Analytic number theory, colloquium publications, vol. 53, American Mathematical Society.
- Kow06 E. Kowalski, Analytic problems for elliptic curves, *J. Ramanujan Math. Soc.* **21** (2006), 19114.
- MPS14 G. Martin, P. Pollack and E. Smith, Averages of the number of points on elliptic curves. *Algebra Number Theory* **8** (2014), no. 4, 813836.
- Par15 J. Parks, Amicable pairs and aliquot cycles on average. *Int. J. Number Theory* **11** (2015), no. 6, 1751-1790.
- Par16 J. Parks, A remark on elliptic curves with a given number of points over finite fields. SCHOLARa scientific celebration highlighting open lines of arithmetic research, 165-179, *Contemp. Math.*, **655**, Amer. Math. Soc., Providence, RI, 2015.
- Rom84 S. Roman, The Umbral Calculus. New York: Academic Press, pp. 59-63, 1984.

Sumit Giri sumit.giri199@gmail.com

School of Mathematics, Tel Aviv University, P.O.B. 39040, Ramat Aviv, Tel Aviv 69978, Israel.